

[Signature]
PATENT
PRO

JC571 U.S. PTO
09/492696
01/27/00

MAY
6/26/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Takashi SHINZAKI et al.**

Serial Number: **Not Yet Assigned**

Filed: **January 27, 2000**

For: **APPARATUS AND METHOD FOR AUTHENTICATING USER
ACCORDING TO BIOMETRIC INFORMATION**

CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Assistant Commissioner for Patents
Washington, D.C. 20231

January 27, 2000

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

Japanese Appln. No. 11-067340, filed on March 12, 1999

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicants have complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI
McLELAND & NAUGHTON

Mel R. Quintos
Mel R. Quintos
Reg. No. 31,898

Atty. Docket No.: 000043
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
Fax: (202) 887-0357
MRQ/yap

JC571 U.S. PRO
09/492696
01/27/00

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the
following application as filed with this Office.

Date of Application: March 12, 1999

Application Number: Patent Application
No. 11-067340

Applicant(s): FUJITSU LIMITED

August 30, 1999

Commissioner,
Patent Office Takeshi Isayama

Certificate No. 11-3060151

日本特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

jc571 U.S. PTO
J 09/492696
n1/27/00


別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application: 1999年 3月12日

出願番号
Application Number: 平成11年特許願第067340号

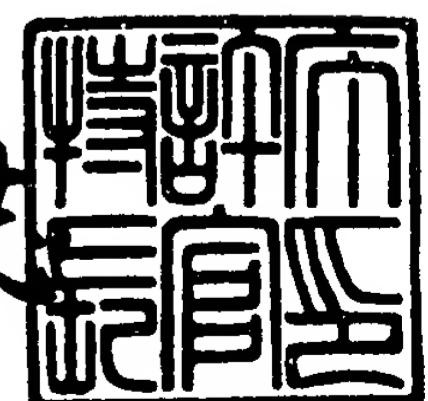
出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 8月30日

特許庁長官
Commissioner
Patent Office

伴佐山達志



出証番号 出証特平11-306015

【書類名】 特許願
【整理番号】 9805170
【提出日】 平成11年 3月12日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 1/00
H04L 9/32
【発明の名称】 生体情報を用いて個人認証を行う認証装置および方法
【請求項の数】 13
【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内
【氏名】 新崎 卓
【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内
【氏名】 藤井 勇作
【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社
【代理人】
【識別番号】 100074099
【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F
【弁理士】
【氏名又は名称】 大菅 義之
【電話番号】 03-3238-0031
【選任した代理人】
【識別番号】 100067987
【住所又は居所】 神奈川県横浜市港北区太尾町1418-305 (大倉
山二番館)

【弁理士】

【氏名又は名称】 久木元 彰

【電話番号】 045-545-9280

【手数料の表示】

【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 生体情報を用いて個人認証を行う認証装置および方法

【特許請求の範囲】

【請求項1】 生体情報を入力する生体情報入力手段と、
入力された生体情報から生体特徴情報を抽出する抽出手段と、
抽出された生体特徴情報の照合精度を推定する推定手段と、
所定の照合精度が得られないと推定されるとき、付加的な認証情報の入力を要
求する要求手段と、
前記認証情報を入力する認証情報入力手段と、
登録生体特徴情報をあらかじめ格納する生体特徴情報登録手段と、
付加的な登録認証情報をあらかじめ格納する認証情報登録手段と、
前記抽出された生体特徴情報と前記登録生体特徴情報を照合する生体特徴情報
照合手段と、
入力された認証情報を前記登録認証情報を照合する認証情報照合手段と、
生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精
度を計算し、計算結果に基づいて本人であるかどうかを判定する判定手段と
を備えることを特徴とする認証装置。

【請求項2】 前記要求手段は、前記認証情報としてパスワード情報を要求
し、前記認証情報入力手段は、該パスワード情報を入力し、前記認証情報登録手
段は、前記登録認証情報として登録パスワード情報をあらかじめ格納し、前記認
証情報照合手段は、入力されたパスワード情報を該登録パスワード情報を照合す
ることを特徴とする請求項1記載の認証装置。

【請求項3】 前記要求手段は、前記所定の照合精度を得るために必要なパ
スワード情報の桁数を設定し、設定された桁数のパスワード情報の入力を要求す
る設定手段を含むことを特徴とする請求項2記載の認証装置。

【請求項4】 生体情報を入力する生体情報入力手段と、
入力された生体情報から生体特徴情報を抽出する抽出手段と、
抽出された生体特徴情報の照合精度を推定する推定手段と、
所定の照合精度が得られないと推定されるとき、他の生体情報の入力を要求す

る要求手段と、

複数の登録生体特徴情報をあらかじめ格納する生体特徴情報登録手段と、
前記抽出された生体特徴情報を前記登録生体特徴情報を照合する生体特徴情報
照合手段と、

入力された複数の生体情報を抽出された複数の生体特徴情報の照合結果を組
み合わせて照合精度を計算し、計算結果に基づいて本人であるかどうかを判定す
る判定手段と

を備えることを特徴とする認証装置。

【請求項5】 生体情報を入力する生体情報入力手段と、
入力された生体情報を抽出する抽出手段と、
付加的な認証情報を入力する認証情報入力手段と、
登録生体特徴情報をあらかじめ格納する生体特徴情報登録手段と、
付加的な登録認証情報をあらかじめ格納する認証情報登録手段と、
前記抽出された生体特徴情報を前記登録生体特徴情報を照合する生体特徴情報
照合手段と、

生体特徴情報の照合結果から所定の照合精度が得られないとき、入力された認
証情報を前記登録認証情報を照合する認証情報照合手段と、

生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精
度を計算し、計算結果に基づいて本人であるかどうかを判定する判定手段と
を備えることを特徴とする認証装置。

【請求項6】 クライアントサーバ型の認証システムにおけるクライアント
装置であって、

生体情報を入力する生体情報入力手段と、
入力された生体情報を抽出する抽出手段と、
抽出された生体特徴情報の照合精度を推定する推定手段と、
所定の照合精度が得られないと推定されるとき、付加的な認証情報の入力を要
求する要求手段と、
前記認証情報を入力する認証情報入力手段と、
前記抽出された生体特徴情報を入力された認証情報を結合して照合データを作

成する作成手段と、

作成された照合データを登録情報と照合するために、該照合データをサーバに送信する通信手段と

を備えることを特徴とするクライアント装置。

【請求項7】 前記照合データ作成手段は、前記抽出された生体特徴情報と前記入力された認証情報の種類情報と、前記照合データのフォーマット情報のうち、少なくとも一方を該照合データに記述することを特徴とする請求項6記載のクライアント装置。

【請求項8】 クライアントサーバ型の認証システムにおけるサーバ装置であって、

生体特徴情報と付加的な認証情報をクライアントから受信する通信手段と、
登録生体特徴情報をあらかじめ格納する生体特徴情報登録手段と、
付加的な登録認証情報をあらかじめ格納する認証情報登録手段と、
受信した生体特徴情報を前記登録生体特徴情報を照合する生体特徴情報照合手段と、

受信した認証情報を前記登録認証情報を照合する認証情報照合手段と、
生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精度を計算し、計算結果に基づいて本人であるかどうかを判定する判定手段とを備えることを特徴とするサーバ装置。

【請求項9】 生体情報を入力する生体情報入力手段と、
入力された生体情報を抽出する抽出手段と、
抽出された生体特徴情報の照合精度を推定する推定手段と、
所定の照合精度が得られないと推定されるとき、付加的な認証情報の入力を要求する要求手段と、
前記認証情報を入力する認証情報入力手段と、
前記生体特徴情報を登録生体特徴情報として格納する生体特徴情報登録手段と

前記認証情報を付加的な登録認証情報として格納する認証情報登録手段と、
認証のために入力された生体情報を抽出された生体特徴情報と前記登録生体

特徴情報を照合する生体特徴情報照合手段と、

認証のために入力された認証情報と前記登録認証情報を照合する認証情報照合手段と、

生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精度を計算し、計算結果に基づいて本人であるかどうかを判定する判定手段とを備えることを特徴とする認証装置。

【請求項10】 クライアントサーバ型の認証システムにおけるクライアント装置であって、

生体情報を入力する生体情報入力手段と、

入力された生体情報から生体特徴情報を抽出する抽出手段と、

抽出された生体特徴情報の照合精度を推定する推定手段と、

所定の照合精度が得られないと推定されるとき、付加的な認証情報の入力を要求する要求手段と、

前記認証情報を入力する認証情報入力手段と、

前記抽出された生体特徴情報を入力された認証情報を結合して登録データを作成する作成手段と、

作成された登録データを登録するために、該登録データをサーバに送信する通信手段と

を備えることを特徴とするクライアント装置。

【請求項11】 クライアントサーバ型の認証システムにおけるサーバ装置であって、

生体特徴情報と付加的な認証情報をクライアントから受信する通信手段と、

受信した生体特徴情報を登録生体特徴情報として格納する生体特徴情報登録手段と、

受信した認証情報を付加的な登録認証情報として格納する認証情報登録手段と

、
認証のためにクライアントから受信した生体特徴情報と前記登録生体特徴情報を照合する生体特徴情報照合手段と、

認証のためにクライアントから受信した認証情報と前記登録認証情報を照合す

る認証情報照合手段と、

生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精度を計算し、計算結果に基づいて本人であるかどうかを判定する判定手段とを備えることを特徴とするサーバ装置。

【請求項12】 各識別情報に対応して格納された登録情報の種類を管理するデータベース手段と、クライアントから受信した識別情報に対応する登録情報の種類を検索する検索手段と、検索された種類に対応する照合情報の入力を該クライアントに要求する要求手段とをさらに備えることを特徴とする請求項11記載のサーバ装置。

【請求項13】 生体情報を取得し、

得られた生体情報から生体特徴情報を抽出し、

抽出された生体特徴情報の照合精度を推定し、

所定の照合精度が得られないと推定されるとき、付加的な認証情報を取得し、

前記抽出された生体特徴情報とあらかじめ登録された登録生体特徴情報を照合し、

得られた認証情報とあらかじめ登録された付加的な登録認証情報を照合し、

生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精度を計算し、

計算結果に基づいて本人であるかどうかを判定することを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、指紋、音声等の生体情報を用いて個人認証を行う認証装置およびその方法に関する。

【0002】

【従来の技術】

現在、通信回線のインフラが整いつつある。コンピュータ等の情報機器が通信回線を介して相互に接続され、ユーザは、遠隔地から様々なサービスを利用でき

るようになった。金銭やプライバシーが絡むサービスでは、パスワード等により本人を確認するプロセスが必須である。

【0003】

反面、自分のコンピュータを使って自動的にパスワードを発見するプログラムを作成できる等、犯罪者にとっても好都合な環境が整いつつある。そこで、長いパスワードの使用が求められているが、管理や記憶が面倒である面は否めない。これに対して、指紋、音声等の生体情報を用いた照合は、管理や記憶の簡単さや本人認証の正確さから、パスワードに替わる方法として期待されている。

【0004】

【発明が解決しようとする課題】

しかしながら、従来の生体情報による個人認証技術には、次のような問題がある。

【0005】

生体情報の再現性は個人差が大きく、特定の個人ではそれがかなり低い場合もある。そのようなユーザにとっては、そのままではシステムの利用が困難である。また、システム的にも、生体情報による個人認証技術の未適用者（利用できない人）への対応が不十分である。

【0006】

さらに、生体情報を用いた個人認証技術では、本人受付率と他人受付率はトレードオフの関係にあり、一定の本人受付率を保つためには他人受付率を上げなければならないという問題が発生する。したがって、特定の生体情報を採用した場合に、その生体情報の利用が困難なユーザに対して、システム的な解決策の提供が必要となる。

【0007】

特に、ネットワーク上における個人認証では、利用困難なユーザに対する例外処理を上手く行わなければ、通常のネットワークプロトコルやシーケンスからの逸脱が生じる。

【0008】

また、既存のパスワードを使用するシステムにおいては、1種類の認証データ

のみが送られるようになっているため、生体情報のような代替手段との切り替えが難しいという問題もある。

【0009】

本発明の課題は、生体情報を用いた個人認証技術において、生体情報の再現性が悪いユーザを含むより多くのユーザが利用可能な認証装置およびその方法を提供することである。

【0010】

【課題を解決するための手段】

図1は、本発明の認証装置の原理図である。

本発明の第1の原理によれば、認証装置は、生体情報入力手段1、抽出手段2、推定手段3、要求手段4、認証情報入力手段5、生体特徴情報登録手段6、認証情報登録手段7、生体特徴情報照合手段8、認証情報照合手段9、および判定手段10を備える。

【0011】

生体情報入力手段1は、生体情報を入力し、抽出手段2は、入力された生体情報から生体特徴情報を抽出し、推定手段3は、抽出された生体特徴情報の照合精度を推定する。所定の照合精度が得られないと推定されるとき、要求手段4は、付加的な認証情報の入力を要求し、認証情報入力手段5は、認証情報を入力する。

【0012】

生体特徴情報登録手段6は、登録生体特徴情報をあらかじめ格納し、認証情報登録手段7は、付加的な登録認証情報をあらかじめ格納する。生体特徴情報照合手段8は、抽出された生体特徴情報と登録生体特徴情報を照合し、認証情報照合手段9は、入力された認証情報と登録認証情報を照合する。そして、判定手段10は、生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて照合精度を計算し、計算結果に基づいて本人であるかどうかを判定する。

【0013】

抽出手段2は、ユーザの生体情報の特徴を表す生体特徴情報を抽出し、推定手段3は、その生体特徴情報の品質から照合精度を推定する。要求手段4は、推定

された照合精度が所定の照合精度より悪いとき、パスワードのような付加的な認証情報の入力をユーザに要求する。また、推定された照合精度が所定の照合精度に達していれば、付加的な認証情報を要求しない。

【0014】

認証情報が入力されると、生体特徴情報照合手段8は、生体特徴情報の照合を行い、認証情報照合手段9は、認証情報の照合を行う。そして、判定手段10は、それらの照合結果を組み合わせて照合精度を計算し、所定の照合精度が得られれば、ユーザを本人と判定し、判定結果を出力する。

【0015】

このような認証装置によれば、照合処理を行う前に生体特徴情報の照合精度が推定されるため、生体特徴情報の再現性が悪いユーザでも、付加的な認証情報を入力して認証を受けることができる。また、生体特徴情報の再現性が良いユーザは、付加的な認証情報を入力する必要がなくなる。

【0016】

また、本発明の第2の原理によれば、認証装置は、生体情報入力手段1、抽出手段2、推定手段3、要求手段4、生体特徴情報登録手段6、生体特徴情報照合手段8、および判定手段10を備える。

【0017】

生体情報入力手段1は、生体情報を入力し、抽出手段2は、入力された生体情報から生体特徴情報を抽出し、推定手段3は、抽出された生体特徴情報の照合精度を推定する。所定の照合精度が得られないと推定されるとき、要求手段4は、他の生体情報の入力を要求する。

【0018】

生体特徴情報登録手段6は、複数の登録生体特徴情報をあらかじめ格納し、生体特徴情報照合手段8は、抽出された生体特徴情報と登録生体特徴情報を照合する。そして、判定手段10は、入力された複数の生体情報から抽出された複数の生体特徴情報の照合結果を組み合わせて照合精度を計算し、計算結果に基づいて本人であるかどうかを判定する。

【0019】

要求手段4は、推定された照合精度が所定の照合精度より悪いとき、先に入力された生体情報と同じ種類または異なる種類の他の生体情報の入力をユーザに要求する。例えば、先に入力された生体情報が指紋情報であれば、他の指の指紋情報または音声等の他の種類の生体情報を要求する。また、推定された照合精度が所定の照合精度に達していれば、他の生体情報を要求しない。

【0020】

生体情報入力手段1が他の生体情報を入力すると、抽出手段2は、その生体情報から生体特徴情報を抽出し、生体特徴情報照合手段8は、複数の生体特徴情報の照合を行う。そして、判定手段10は、それらの照合結果を組み合わせて照合精度を計算し、所定の照合精度が得られれば、ユーザを本人と判定し、判定結果を出力する。

【0021】

このような認証装置によれば、照合処理を行う前に生体特徴情報の照合精度が推定されるため、生体特徴情報の再現性が悪いユーザでも、他の生体情報を入力して認証を受けることができる。また、生体特徴情報の再現性が良いユーザは、他の生体情報を入力する必要がなくなる。

【0022】

以上説明したように、本発明の1つのポイントは、生体特徴情報の照合処理を行う前にその照合精度を推定し、推定結果に基づいて、パスワードや他の生体情報のような付加的な認証情報の入力を要求することである。また、本発明のもう1つのポイントは、生体特徴情報の照合結果と付加的な認証情報の照合結果を組み合わせて判定を行うことである。

【0023】

例えば、図1の生体情報入力手段1、抽出手段2、推定手段3、認証情報入力手段5、生体特徴情報登録手段6、認証情報登録手段7、生体特徴情報照合手段8、認証情報照合手段9、および判定手段10は、それぞれ、後述する生体情報入力部、生体特徴情報抽出部、照合精度推定部、補助情報入力部、生体特徴情報登録保存部、補助情報登録保存部、生体特徴情報照合部、補助情報照合部、および照合結果判定部に対応する。また、図1の要求手段4は、例えば、後述する補

助情報設定部または生体情報設定部に対応する。

【0024】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

本発明においては、生体情報による個人認証が困難な人に対して、次のようなインターフェースを提供する。

- (1) 認証情報の登録時に、生体情報の特徴を表す生体特徴情報以外に付加的な認証データを登録する。
- (2) 認証情報の登録時に、登録データの照合精度（本人受付率、他人受付率等）を判断し、付加的な認証データの登録を促す。
- (3) 認証情報の照合時に、照合データの照合精度（本人受付率、他人受付率等）を判断し、付加的な認証データの入力を促す。
- (4) 生体特徴情報と付加的な認証データを1つの照合データとして扱うことで、通信の手順を1種類にする。

【0025】

生体情報としては、指紋、目の虹彩、声紋、網膜血管分布、署名のように、ユーザの生体の性質に基づく任意の情報が用いられる。生体情報の種類は用いられる照合方法によって異なるが、例えば、指紋の場合は、指紋画像や指紋画像から抽出された生体キー情報等が生体情報として入力される。また、付加的な認証データとしては、パスワードのような補助情報、別の生体特徴情報等が用いられる。

【0026】

このようなインターフェースを備えることで、生体特徴情報の再現性が悪いユーザでも、付加的な認証データを入力して認証システムを利用することができる。また、生体特徴情報と付加的な認証データを1つの照合データとして扱うため、クライアントサーバ型の照合システムにおいては、パスワードによる照合と同様の通信手順を使用することができる。以下では、本発明による認証装置／システムの様々な実施形態について、順に説明する。

【0027】

第1の認証装置は、登録の際に、生体特徴情報と生体特徴情報以外の補助情報を登録し、照合時に、まず、生体情報の入力をユーザに求める。そして、生体情報から抽出された生体特徴情報の品質から所定の照合精度が得られないと判断した場合に、補助情報の入力をユーザに求める。

【0028】

補助情報としては、本人しか知らない秘密情報、個人情報、パスワード等が用いられる。また、ユーザは、磁気カード、IC (integrated circuit) カード、非接触カード等の任意の媒体に補助情報を記録しておき、その媒体を介して補助情報を入力することもできる。媒体を利用することで、ユーザは補助情報を記憶する必要がなくなる。また、照合に用いる補助情報は1つとは限らず、複数の補助情報を併用してもよい。

【0029】

例えば、風邪をひいている場合の音声照合や、指が荒れている場合の指紋照合等において、生体情報が変動を受けた場合や生体特徴情報の再現性が悪いでも、補助情報の入力を要求することで、所定の照合精度の照合結果が得られる。したがって、生体情報が使用不可能になることなく、本人確認が容易に行われる。

【0030】

また、照合時に生体特徴情報の照合精度を推定することで、補助情報の入力要求を必要最低限にすることができる。したがって、生体特徴情報の再現性が良いユーザは、補助情報の入力を省略することができる。

【0031】

図2は、このような認証装置の構成図である。図2の認証装置は、生体情報入力部11、生体特徴情報抽出部12、照合精度推定部13、補助情報設定部14、補助情報入力部15、照合部16、照合結果判定部17、保存部18、および制御部19を備える。照合部16は、生体特徴情報照合部20と補助情報照合部21を含み、保存部18は、生体特徴情報登録保存部22と補助情報登録保存部23を含む。

【0032】

制御部19は、装置全体の動作を制御する。生体情報入力部11は、生体情報

を入力し、生体特徴情報抽出部12は、入力された生体情報から生体特徴情報を抽出する。照合精度推定部13は、照合時に入力された生体情報から抽出された生体特徴情報の品質から照合精度を推定し、所定の照合精度が得られないと判断した場合は、認証のための補助情報が必要であることを補助情報設定部14に通知する。これを受け、補助情報設定部14は、ユーザに補助情報の入力を促し、補助情報入力部15は、補助情報を入力する。

【0033】

例えば、生体情報として指紋画像が入力された場合、生体特徴情報を抽出することにより、指紋画像の輝度、コントラスト、誤特徴点を含む特徴点数、指紋隆線の亀裂数、指紋隆線の輪郭線長、周波数成分、検出された隆線方向情報の乱れ、入力画像の面積等の情報が得られる。そこで、これらの情報に基づいて、照合精度が判定される。

【0034】

生体特徴情報登録保存部22には、あらかじめ生体情報から抽出された生体特徴情報を登録保存しておき、補助情報登録保存部23には、あらかじめ補助情報を登録保存しておく。生体特徴情報照合部20は、入力された生体特徴情報とあらかじめ登録された生体特徴情報を照合し、補助情報照合部21は、入力された補助情報とあらかじめ登録された補助情報を照合する。

【0035】

照合結果判定部17は、生体特徴情報の照合結果（スコア）から算出される照合精度と補助情報の照合結果から算出される照合精度を、所定の関数により組み合わせて計算し、所定の精度以上の照合精度が得られた場合に、本人と認証する。

【0036】

ここで、照合精度として他人受付率（誤照合率）が用いられ、所定の関数として2つの他人受付率の積が用いられた場合を考えてみる。生体特徴情報の照合スコアと他人受付率の関係が図3のように設定され、補助情報の照合スコアと他人受付率の関係が図4のように設定され、本人認証のために必要な他人受付率の基準値が $1/100000$ に設定されているとする。

【0037】

生体特徴情報の照合により得られたスコアが“4”であり、補助情報の照合により得られたスコアが“14”である場合、図3、4より、対応する他人受付率はそれぞれ $1/1000$ 、 $1/100$ となる。このとき、これらの他人受付率の積は $1/1000 \times 1/100 = 1/100000$ となり、設定された基準値に一致する。したがって、本人と認証される。

【0038】

また、生体特徴情報の照合により得られたスコアが“4”であり、補助情報の照合により得られたスコアが“15”である場合は、図3、4より、対応する他人受付率はそれぞれ $1/1000$ 、 $1/10$ となる。このとき、これらの他人受付率の積は $1/1000 \times 1/10 = 1/10000$ となり、設定された基準値 $1/100000$ より大きくなる。したがって、他人である可能性が高いため、本人ではないと判定される。

【0039】

ここでは、照合精度として他人受付率を用いているが、代わりに本人受付率、他人排除率等の任意の指標を用いることができる。また、所定の関数としてはより複雑な計算式を用いることもでき、照合スコアと照合精度の関係を表すテーブルをより精密に設定することもできる。

【0040】

図5は、図2の認証装置による認証処理のフローチャートである。まず、生体情報入力部11はユーザの生体情報を入力し（ステップS1）、生体特徴情報抽出部12は生体情報から生体特徴情報を抽出する（ステップS2）。次に、照合精度推定部13は、生体特徴情報の品質から照合精度を推定し（ステップS3）、推定された照合精度を所定の照合精度と比較する（ステップS4）。

【0041】

推定された照合精度が所定の照合精度以上であれば、生体特徴情報照合部20は、抽出された生体特徴情報と生体特徴情報登録保存部22に登録された生体特徴情報を照合し（ステップS5）、照合結果を所定の一致閾値と比較する（ステップS6）。そして、照合結果が閾値以上であれば本人と判断し（ステップS7

)、照合結果が閾値未満であれば他人と判断して(ステップS8)、処理を終了する。

【0042】

また、ステップS4において、推定された照合精度が所定の照合精度未満であれば、補助情報設定部14はユーザに補助情報の入力を要求し(ステップS9)、補助情報入力部15は補助情報を入力する(ステップS10)。

【0043】

次に、生体特徴情報照合部20は、抽出された生体特徴情報と生体特徴情報登録保存部22に登録された生体特徴情報を照合し(ステップS11)、補助情報照合部21は、入力された補助情報と補助情報登録保存部23に登録された補助情報を照合する(ステップS12)。

【0044】

次に、照合結果判定部17は、生体特徴情報の照合結果と補助情報の照合結果を用いて組み合わせ演算を行い(ステップS13)、得られた演算値を所定の一一致閾値と比較する(ステップS14)。そして、演算値が閾値以上であれば本人と判断し(ステップS15)、演算値が閾値未満であれば他人と判断して(ステップS16)、処理を終了する。

【0045】

次に、第2の認証装置は、登録の際に、生体特徴情報と生体特徴情報以外の補助情報を登録し、照合時に、生体情報の入力をユーザに求め、生体特徴情報の品質を判断する。そして、所定の照合精度が得られないと判断した場合に、パスワードの入力をユーザに求める。生体特徴情報の照合精度が悪い場合に、パスワードの照合精度と組み合わせることで、補助情報を用いた場合と同様にして所定の照合精度の達成が図られる。

【0046】

このとき、入力パスワードの桁数を可変にしておき、第2の認証装置は、生体特徴情報の照合精度と組み合わせて所定の照合精度を達成するために必要な桁数のパスワードの入力を求める。ユーザは必要最低限の桁数のパスワードを入力すればよいので、生体特徴情報による利便性が損なわれない。

【0047】

図6は、このような認証装置の構成図である。図6の認証装置は、生体情報入力部31、生体特徴情報抽出部32、照合精度推定部33、パスワード情報設定部34、パスワード桁数設定部35、パスワード情報入力部36、照合部37、照合結果判定部38、保存部39、および制御部40を備える。照合部37は、生体特徴情報照合部41とパスワード情報照合部42を含み、保存部39は、生体特徴情報登録保存部43とパスワード情報登録保存部44を含む。

【0048】

生体情報入力部31、生体特徴情報抽出部32、照合精度推定部33、生体特徴情報照合部41、生体特徴情報登録保存部43、および制御部40の動作は、図2の認証装置の場合と同様である。

【0049】

照合精度推定部33は、生体特徴情報から所定の照合精度が得られないと判断した場合は、照合精度の不足分を補うために必要なパスワードの桁数をパスワード情報設定部34に通知する。これを受けて、パスワード情報設定部34は、その桁数をパスワード桁数設定部35に入力し、パスワード桁数設定部35は、その桁数を設定して、その桁数以上のパスワードの入力をユーザに促す。そして、パスワード情報入力部36は、パスワード情報を入力する。

【0050】

パスワード情報登録保存部44には、あらかじめパスワード情報を登録保存しておく。パスワード情報照合部42は、入力されたパスワード情報とあらかじめ登録されたパスワード情報を照合する。

【0051】

照合結果判定部38は、生体特徴情報の照合結果から算出される照合精度とパスワード情報の照合結果から算出される照合精度を、所定の関数により組み合わせて計算し、所定の精度以上の照合精度が得られた場合に、本人と認証する。

【0052】

例えば、照合精度として他人受付率が用いられ、所定の関数として2つの他人受付率の積が用いられ、本人認証のために必要な他人受付率の基準値が $1/10$

0000に設定されているとする。そして、生体特徴情報では1/1000の照合精度しか得られないと推定され、マージンをみて3桁のパスワードの入力が要求されたとする。

【0053】

このとき、生体特徴情報を実際に照合してみて、1/1000の他人受付率が得られれば、組み合わせ演算により、パスワードの他人受付率は1/10以下でよいことになる。したがって、入力された全桁が必ずしも登録パスワードと一致する必要はなく、1桁または2桁が一致しただけで本人と認証することもできる。

【0054】

図7は、図6の認証装置による認証処理のフローチャートである。図7のステップS21からS28までの処理については、図5のステップS1からS8までの処理と同様である。

【0055】

ステップS24において、推定された照合精度が所定の照合精度未満であれば、パスワード桁数設定部35は、必要なパスワードの桁数を設定し（ステップS29）、ユーザにパスワード情報の入力を要求する（ステップS30）。そして、パスワード情報入力部36はパスワード情報を入力する（ステップS31）。

【0056】

次に、生体特徴情報照合部41は、抽出された生体特徴情報と生体特徴情報登録保存部43に登録された生体特徴情報を照合し（ステップS32）、パスワード情報照合部42は、入力されたパスワード情報とパスワード情報登録保存部44に登録されたパスワード情報を照合する（ステップS33）。

【0057】

次に、照合結果判定部38は、生体特徴情報の照合結果とパスワード情報の照合結果を用いて組み合わせ演算を行い（ステップS34）、得られた演算値を所定の一致閾値と比較する（ステップS35）。そして、演算値が閾値以上であれば本人と判断し（ステップS36）、演算値が閾値未満であれば他人と判断して（ステップS37）、処理を終了する。

【0058】

次に、第3の認証装置は、複数個の生体特徴情報を登録しておき、それらを用いて認証処理を行う。例えば、生体情報が指紋の場合は、左右の人指し指の指紋を用い、虹彩の場合は右目と左目の情報を用い、音声の場合は複数の異なるフレーズまたは母音を用い、署名の場合は複数の異なるサインを用いる。

【0059】

第3の認証装置は、照合時に、生体情報の入力をユーザに求め、生体特徴情報の品質を判断する。そして、所定の照合精度が得られないと判断した場合は、登録してある他の生体特徴情報に対応する生体情報の入力を求める。複数個の生体情報を用いるため、パスワード等を記憶する必要がなく、生体情報のみで確実な本人認証を行うことができる。

【0060】

図8は、生体情報として指紋を用いた場合の認証装置の構成図である。図8の認証装置は、指紋情報入力部51、指紋特徴情報抽出部52、照合精度推定部53、照合部54、照合結果判定部55、保存部56、および制御部57を備える。照合部54は、指紋特徴情報照合部58を含み、保存部56は、指紋特徴情報登録保存部59を含む。

【0061】

制御部57は、装置全体の動作を制御する。指紋情報入力部51は、指紋画像を入力し、指紋特徴情報抽出部52は、入力された指紋画像から指紋特徴情報を抽出する。照合精度推定部53は、照合時に入力された指紋画像から抽出された指紋特徴情報の品質から照合精度を推定し、所定の照合精度が得られないと判断した場合は、他の指の指紋画像との併用が必要であることを制御部57に通知する。これを受け、制御部57は、ユーザに登録済みの他の指の指紋画像の入力を促し、指紋情報入力部51は、その指紋画像を入力する。

【0062】

例えば、最初に右人指し指の指紋画像が入力されたが、照合精度が不足すると推定された場合、次に右中指の指紋画像の入力が要求される。

指紋特徴情報登録保存部59には、あらかじめ複数の指の指紋画像から抽出さ

れた指紋特徴情報を登録保存しておく。指紋特徴情報照合部58は、入力された複数の指の指紋特徴情報と指紋特徴情報登録保存部59の対応する指紋特徴情報を照合する。

【0063】

照合結果判定部55は、各指の指紋特徴情報の照合結果から算出される照合精度を所定の閾数により組み合わせて計算し、所定の精度以上の照合精度が得られた場合に、本人と認証する。

【0064】

このように、1つの指の指紋特徴情報では照合精度が落ちると推定された場合に、複数の指の指紋特徴情報を併用することで、所定の照合精度を得ることができる。

【0065】

図9は、図8の認証装置による認証処理のフローチャートである。まず、指紋情報入力部51はユーザの第1の指の指紋情報を入力し（ステップS41）、指紋特徴情報抽出部52は第1の指紋情報をから第1の指紋特徴情報を抽出する（ステップS42）。次に、照合精度推定部53は、指紋特徴情報の品質から照合精度を推定し（ステップS43）、推定された照合精度を所定の照合精度と比較する（ステップS44）。

【0066】

推定された照合精度が所定の照合精度以上であれば、指紋特徴情報照合部58は、抽出された指紋特徴情報と指紋特徴情報登録保存部59に登録された指紋特徴情報を照合し（ステップS45）、照合結果を所定の一致閾値と比較する（ステップS46）。そして、照合結果が閾値以上であれば本人と判断し（ステップS47）、照合結果が閾値未満であれば他人と判断して（ステップS48）、処理を終了する。

【0067】

また、ステップS44において、推定された照合精度が所定の照合精度未満であれば、制御部57はユーザに第2の指の指紋情報の入力を要求する（ステップS49）。そして、指紋情報入力部51は第2の指紋情報を入力し（ステップS

50)、指紋特徴情報抽出部52は第2の指紋情報から第2の指紋特徴情報を抽出する(ステップS51)。

【0068】

次に、指紋特徴情報照合部54は、第1の指紋特徴情報と指紋特徴情報登録保存部22に登録された対応する指紋特徴情報を照合し(ステップS52)、第2の指紋特徴情報と指紋特徴情報登録保存部22に登録された対応する指紋特徴情報を照合する(ステップS53)。

【0069】

次に、照合結果判定部55は、2つの指紋特徴情報の照合結果を用いて組み合わせ演算を行い(ステップS54)、得られた演算値を所定の一致閾値と比較する(ステップS55)。そして、演算値が閾値以上であれば本人と判断し(ステップS56)、演算値が閾値未満であれば他人と判断して(ステップS57)、処理を終了する。

【0070】

ここでは、指紋を用いて説明したが、虹彩(左右の目)、声紋(異なるフレーズ、母音)、網膜血管分布(左右の目)、署名(異なるサイン)等の他の生体情報を用いた場合も同様である。また、人差し指、中指、および親指のように、3つ以上の生体情報を用いた場合も同様である。

【0071】

次に、第4の認証装置は、照合方法の異なる複数種類の生体特徴情報を登録しておき、複数の照合方法を組み合わせて認証処理を行う。例えば、指紋と音声、指紋と虹彩、音声と虹彩、指紋と署名、指紋と顔等の組合せが用いられる。

【0072】

第4の認証装置は、照合時に、生体情報の入力をユーザに求め、生体特徴情報の品質を判断する。そして、所定の照合精度が得られないと判断した場合は、登録してある他の種類の生体特徴情報に対応する生体情報の入力を求める。複数種類の照合方法を用いるため、パスワード等を記憶する必要がなく、生体情報のみで確実な本人認証を行うことができる。

【0073】

図10は、このような認証装置の構成図である。図10の認証装置は、生体情報入力部61、65、生体特徴情報抽出部62、66、照合精度推定部63、生体情報設定部64、照合部67、照合結果判定部68、保存部69、および制御部70を備える。照合部67は、生体特徴情報照合部71、72を含み、保存部69は、生体特徴情報登録保存部73、74を含む。

【0074】

生体情報入力部61、生体特徴情報抽出部62、照合精度推定部63、および制御部70の動作は、図2の認証装置の場合と同様である。

照合精度推定部63は、生体特徴情報から所定の照合精度が得られないと判断した場合は、他の照合方法との併用が必要であることを生体情報設定部64に通知する。これを受け、生体情報設定部64は、他の種類の生体情報を設定し、その生体情報の入力をユーザに促す。例えば、最初に指紋情報が入力されたが、照合精度が不足すると推定された場合、次に音声情報の入力が要求される。

【0075】

生体情報入力部65は、生体情報を入力し、生体特徴情報抽出部66は、入力された生体情報から生体特徴情報を抽出する。

生体特徴情報登録保存部73、74には、それぞれ異なる種類の生体特徴情報をあらかじめ登録保存しておく。生体特徴情報照合部71は、生体特徴情報抽出部62により抽出された生体特徴情報を生体特徴情報登録保存部73の生体特徴情報を照合し、生体特徴情報照合部72は、生体特徴情報抽出部66により抽出された生体特徴情報を生体特徴情報登録保存部74の生体特徴情報を照合する。一般に、生体特徴情報照合部71、72は、それぞれ異なる照合方法を用いて生体特徴情報を照合する。

【0076】

照合結果判定部68は、生体特徴情報照合部71、72による照合結果からそれぞれ算出される照合精度を所定の関数により組み合わせて計算し、所定の精度以上の照合精度が得られた場合に、本人と認証する。

【0077】

図11は、図10の認証装置による認証処理のフローチャートである。図11

のステップS61からS68までの第1の生体情報に関する処理については、図5のステップS1からS8までの処理と同様である。

【0078】

ステップS64において、推定された照合精度が所定の照合精度未満であれば、生体情報設定部64は、第1の生体情報とは異なる種類の第2の生体情報の入力をユーザに要求する（ステップS69）。そして、生体情報入力部65は第2の生体情報を入力し（ステップS70）、生体特徴情報抽出部66は第2の生体情報から第2の生体特徴情報を抽出する（ステップS71）。

【0079】

次に、生体特徴情報照合部71は、第1の生体特徴情報と生体特徴情報登録保存部73に登録された生体特徴情報を照合し（ステップS72）、生体特徴情報照合部72は、第2の生体特徴情報と生体特徴情報登録保存部74に登録された生体特徴情報を照合する（ステップS73）。

【0080】

次に、照合結果判定部68は、2種類の生体特徴情報の照合結果を用いて組み合わせ演算を行い（ステップS74）、得られた演算値を所定の一致閾値と比較する（ステップS75）。そして、演算値が閾値以上であれば本人と判断し（ステップS76）、演算値が閾値未満であれば他人と判断して（ステップS77）、処理を終了する。

【0081】

ここでは、第1および第2の生体情報として、指紋、虹彩、声紋、網膜血管分布、署名等の異なる種類の生体情報の任意の組合せを用いることができる。また、指紋、虹彩、および声紋のように、3種類以上の生体情報を用いた場合も同様である。

【0082】

ところで、図2および図6の認証装置においては、生体特徴情報とパスワード等の補助情報がそれぞれ別の照合データとして照合部に入力されているが、これらの情報を1つの照合データとしてまとめて照合部に送ることも可能である。装置内部で照合データをまとめて扱うことで、照合経路がシンプルになる。つまり

、生体特徴情報抽出部および補助情報入力部から照合部には、1種類の照合データを1回転送するだけで済む。また、多種類の照合データを入力するフェーズを繰り返す必要がなくなる。

【0083】

そこで、認証装置に照合データ作成部を設けることにする。生体特徴情報の品質から所定の照合精度が得られないと判断した場合は、照合データ作成部が、生体特徴情報と補助情報を結合して、図12に示すような1つの照合データを作成し、照合部へ送る。

【0084】

図13は、認証装置による照合データ作成処理のフローチャートである。認証装置は、まず、生体情報を入力し（ステップS81）、生体情報から生体特徴情報を抽出し（ステップS82）、補助情報を入力する（ステップS83）。次に、補助情報のデータ処理を行い（ステップS84）、生体特徴情報と補助情報を結合して照合データを作成して（ステップS85）、処理を終了する。

【0085】

同様にして、図8の認証装置においては、複数の指の指紋特徴情報を結合して1つの照合データを作成することができる。より一般的には、同一の照合方法に対応する複数個の生体特徴情報を結合して1つの照合データを作成することができる。また、図10の認証装置においては、照合方法の異なる複数種類の生体特徴情報を結合して1つの照合データを作成することができる。これらの照合データを用いれば、照合経路がシンプルになる。

【0086】

このように、複数の照合データの固まりを1つの照合データとして照合部に送り込むことで、既存システムとの連携時に従来通りの1種類の照合データのやりとりで済ませることができ、装置の実装が簡単になる。これに対して、1つの照合データの照合が失敗した場合に次の照合データを要求する方法を採用すれば、通信のコストが2倍以上になると考えられる。

【0087】

次に、クライアントからサーバに生体特徴情報を送信し、サーバで照合を行う

クライアントサーバ型の認証システムについて説明する。このシステムでは、クライアント側で生体特徴情報の照合精度を推定し、必要であれば補助情報の入力を要求する。そして、生体特徴情報と補助情報を結合して照合データを生成し、サーバに送信する。

【0088】

このようなシステムによれば、照合データをサーバに送る回数は1回で済む。また、補助情報を必要とする場合としない場合とで照合データの送信回数が変わらないため、通信手順がシンプルになる。

【0089】

図14は、このような認証システムの構成図である。図14の認証システムは、クライアント81、サーバ82、およびそれらを接続するネットワークシステム83を備える。ネットワークシステム83は、LAN (local area network)、WAN (wide area network) 等の任意のネットワークを含む。

【0090】

クライアント81は、生体情報入力部91、生体特徴情報抽出部92、照合精度推定部93、補助情報設定部94、補助情報入力部95、照合データ作成部96、通信部97、および制御部98を備える。

【0091】

サーバ82は、通信部101、照合部102、照合結果判定部103、保存部104、および制御部105を備える。照合部102は、生体特徴情報照合部106、照合データ分離部107、および補助情報照合部108を含み、保存部104は、生体特徴情報登録保存部109と補助情報登録保存部110を含む。

【0092】

生体情報入力部91、生体特徴情報抽出部92、照合精度推定部93、補助情報設定部94、補助情報入力部95、照合結果判定部103、生体特徴情報照合部106、補助情報照合部108、生体特徴情報登録保存部109、および補助情報登録保存部110の動作は、図2の認証装置の場合と同様である。

【0093】

制御部98は、クライアント81全体の動作を制御し、制御部105は、サー

バ82全体の動作を制御する。クライアント81の照合データ作成部96は、生体特徴情報と補助情報を結合して照合データを作成し、通信部97は、作成された照合データをサーバ82に送信する。サーバ82の通信部101は、照合データを受信する。そして、照合データ分離部107は、照合データを生体特徴情報と補助情報に分解し、生体特徴情報を生体特徴情報照合部106に入力し、補助情報を補助情報照合部108に入力する。

【0094】

図15は、図14のクライアント81の処理のフローチャートである。図15のステップS91からS94までの処理については、図5のステップS1からS4までの処理と同様である。また、図15のステップS97、S98の処理については、図5のステップS9、S10の処理と同様である。

【0095】

ステップS94において、推定された照合精度が所定の照合精度以上であれば、照合データ作成部96は、生体特徴情報のみを含む照合データを作成し（ステップS95）、通信部97は、その照合データをサーバ82に送信して（ステップS96）、処理を終了する。

【0096】

また、ステップS98において補助情報が入力されると、照合データ作成部96は、補助情報のデータ処理を行い（ステップS99）、生体特徴情報と補助情報を結合して照合データを作成する（ステップS100）。そして、通信部97は、その照合データをサーバ82に送信して（ステップS101）、処理を終了する。

【0097】

図16は、図14のサーバ82が生体特徴情報のみを含む照合データを受信した場合の処理のフローチャートである。まず、通信部101は、クライアント81から照合データを受信する（ステップS111）。次のステップS112からS115までの処理については、図5のステップS5からS8までの処理と同様である。

【0098】

図17は、図14のサーバ82が生体特徴情報と補助情報を含む照合データを受信した場合の処理のフローチャートである。まず、通信部101は、クライアント81から照合データを受信し（ステップS121）、照合データ分離部107は、照合データを生体特徴情報と補助情報に分解する（ステップS122）。次のステップS123からS128までの処理については、図5のステップS11からS16までの処理と同様である。

【0099】

同様にして、同一の照合方法に対応する複数個の生体特徴情報を結合して照合データを作成し、クライアントからサーバに送信することもできる。また、照合方法の異なる複数種類の生体特徴情報を結合して照合データを作成し、クライアントからサーバに送信することもできる。

【0100】

このように、複数の照合データを併用する際に、それらを1つの固まりとしてクライアントからサーバに転送することで、通信手順をシンプルにすることがができる。転送された照合データは、サーバ内部で元の照合データに分解されて、それぞれの照合方法に対応する照合部に送られる。これに対して、1つの照合データの照合が失敗した場合に次の照合データを要求する方法を採用すれば、通信のコストが2倍以上になると考えられる。

【0101】

次に、第5の認証装置は、登録の際に、生体特徴情報から予測される照合精度を推定し、所定の照合精度が得られないと判断した場合に、補助情報の登録を求める。そして、照合時に、生体特徴情報と補助情報の照合結果を総合的に判断して、本人確認を行う。生体特徴情報の照合精度と補助情報の照合精度を組み合わせることで、所定の照合精度の達成が図られ、照合失敗の確率が最小限に抑えられる。

【0102】

図18は、このような認証装置の構成図である。図18の認証装置は、生体情報入力部111、生体特徴情報抽出部112、照合精度推定部113、補助情報設定部114、補助情報入力部115、保存部116、照合部117、照合結果

判定部118、および制御部119を備える。保存部116は、生体特徴情報登録保存部120と補助情報登録保存部121を含み、照合部117は、生体特徴情報照合部122と補助情報照合部123を含む。

【0103】

生体情報入力部111、生体特徴情報抽出部112、生体特徴情報登録保存部120、補助情報登録保存部121、生体特徴情報照合部122、補助情報照合部123、照合結果判定部118、および制御部119の動作は、図2の認証装置の場合と同様である。

【0104】

照合精度推定部113は、登録時に入力された生体情報から抽出された生体特徴情報の品質から照合精度を推定し、所定の照合精度が得られないと判断した場合は、認証のための補助情報が必要であることを補助情報設定部114に通知する。これを受け、補助情報設定部114は、ユーザに補助情報の登録を促し、補助情報入力部115は、補助情報を入力する。

【0105】

例えば、登録された指紋特徴情報が少ない場合でも、補助的にパスワードの登録を要求することで、照合時に所定の照合精度を得ることが可能になる。したがって、良好な指紋特徴情報が登録されていないユーザでも、本人として確認されるようになる。

【0106】

図19は、図18の認証装置による登録処理のフローチャートである。図19のステップS131からS134までの処理については、図5のステップS1からS4までの処理と同様である。また、図19のステップS137、S138の処理については、図5のステップS9、S10の処理と同様である。

【0107】

ステップS134において、推定された照合精度が所定の照合精度以上であれば、照合精度推定部113は、生体特徴情報の登録データを作成し（ステップS135）、それを生体特徴情報登録保存部120に登録保存して（ステップS136）、処理を終了する。

【0108】

また、ステップS138において補助情報が入力されると、補助情報入力部115は、補助情報のデータ処理を行い（ステップS139）、補助情報の登録データを作成する（ステップS140）。また、照合精度推定部113は、生体特徴情報の登録データを作成する。そして、照合精度推定部113は、生体特徴情報の登録データを生体特徴情報登録保存部120に登録保存し、補助情報入力部115は、補助情報の登録データを補助情報登録保存部121に登録保存して（ステップS141）、処理を終了する。

【0109】

図20は、図18の認証装置による補助情報を用いた認証処理のフローチャートである。まず、生体情報入力部111は、ユーザに生体情報の入力を要求して（ステップS151）、それを入力し（ステップS152）、生体特徴情報抽出部112は生体情報から生体特徴情報を抽出する（ステップS153）。

【0110】

次に、補助情報入力部115は、ユーザに補助情報の入力を要求し（ステップS154）、それを入力して（ステップS155）、補助情報のデータ処理を行う（ステップS156）。次のステップS157からS162までの処理については、図5のステップS11からS16までの処理と同様である。

【0111】

特に、補助情報としてパスワード情報を用いた場合、補助情報設定部134は、生体特徴情報だけでは不足する照合精度を補うために必要な桁数を設定し、その桁数以上のパスワード情報の登録をユーザに求める。必要最低限の桁数のパスワードを登録することで、生体特徴情報による利便性を損なわずに、確実な認証を行うことができる。逆に、ユーザがパスワードを忘れた場合に、生体情報で補う方法も考えられる。

【0112】

また、生体特徴情報と補助情報を登録する代わりに、複数個の生体特徴情報を登録することもできる。例えば、指紋を用いる場合は、複数指の指紋特徴情報を登録する。認証装置は、登録時に生体特徴情報の品質を判断し、所定の照合精度

が得られないと判断した場合は、他の生体特徴情報の登録を求める。照合時には、各生体特徴情報の照合スコアから総合スコアを計算して、本人確認を行う。これにより、照合失敗の確率が最小限に抑えられる。

【0113】

さらに、照合方法の異なる複数種類の生体特徴情報を登録することもできる。認証装置は、登録時に生体特徴情報の品質を判断し、所定の照合精度が得られないと判断した場合は、他の種類の生体特徴情報の登録を求める。複数種類の照合方法に対応することで、1種類の生体特徴情報の再現性の悪さをカバーすることができる。照合時には、各照合方法の照合結果を総合的に判断して、本人確認を行う。これにより、照合失敗の確率が最小限に抑えられる。

【0114】

次に、第6の認証装置は、生体特徴情報と補助情報を1つの登録データとして登録保存する。装置内で登録データをまとめて扱うことで、データ管理をよりシンプルにすることができる。

【0115】

図21は、このような認証装置の構成図である。図21の認証装置は、生体情報入力部131、生体特徴情報抽出部132、照合精度推定部133、補助情報設定部134、補助情報入力部135、保存部136、照合部137、照合結果判定部138、および制御部139を備える。保存部136は、登録データ作成部140、登録データ保存部141、および登録データ分離部142を含み、照合部137は、生体特徴情報照合部143と補助情報照合部144を含む。

【0116】

生体情報入力部131、生体特徴情報抽出部132、照合精度推定部133、補助情報設定部134、補助情報入力部135、生体特徴情報照合部143、補助情報照合部144、照合結果判定部138、および制御部139の動作は、図18の認証装置の場合と同様である。

【0117】

登録データ作成部140は、生体特徴情報と補助情報を結合して1つの登録データを作成し、登録データ保存部141に登録保存する。登録データ分離部14

2は、登録データ保存部141に登録された登録データを生体特徴情報と補助情報に分解して、照合部137へ送る。

【0118】

図21の認証装置は、図19と同様の登録処理を行う。図19のステップS134において、推定された照合精度が所定の照合精度以上であれば、登録データ作成部140は、生体特徴情報のみを含む登録データを作成し（ステップS135）、それを登録データ保存部141に登録保存して（ステップS136）、処理を終了する。

【0119】

また、ステップS138において補助情報が入力されると、登録データ作成部140は、補助情報のデータ処理を行い（ステップS139）、生体特徴情報と補助情報を結合して登録データを作成する（ステップS140）。そして、登録データを登録データ保存部141に登録保存して（ステップS141）、処理を終了する。

【0120】

同様にして、同一の照合方法に対応する複数個の生体特徴情報を結合して登録データを作成することもでき、照合方法の異なる複数種類の生体特徴情報を結合して登録データを作成することもできる。

【0121】

次に、第7の認証装置は、生体特徴情報を個人識別情報と対応させて登録照合処理を行う場合に、補助情報の種類も登録しておく。そして、照合時に個人識別情報が入力されると、生体情報の入力を要求するとともに、登録された所定の補助情報の入力も要求する。

【0122】

図22は、このような認証装置の構成図である。図22の認証装置は、ID番号入力部151、生体情報入力部152、生体特徴情報抽出部153、照合精度推定部154、補助情報設定部155、補助情報入力部156、保存部157、照合部158、照合結果判定部159、および制御部160を備える。

【0123】

保存部157は、登録データ種類管理部161、ID番号管理部162、登録データ作成部163、登録データ保存部164、および登録データ分離部165を含み、照合部158は、生体特徴情報照合部166と補助情報照合部167を含む。

【0124】

生体情報入力部152、生体特徴情報抽出部153、照合精度推定部154、補助情報設定部155、補助情報入力部156、登録データ作成部163、登録データ保存部164、登録データ分離部165、生体特徴情報照合部166、補助情報照合部167、照合結果判定部159、および制御部160の動作は、図21の認証装置の場合と同様である。

【0125】

登録データ種類管理部161とID番号管理部162は、ユーザの登録ID番号と登録データの種類の対応関係を登録したデータベースに対応する。登録データ作成部163が登録データを登録データ保存部164に登録したとき、登録データ種類管理部161には、登録データに含まれる補助情報の種類が登録され、ID番号管理部162には、対応するID番号が登録される。

【0126】

照合時にID番号入力部151がユーザのID番号を入力すると、登録データ種類管理部161は、そのID番号に対応する補助情報の種類を補助情報設定部155に通知し、補助情報設定部155は、通知された補助情報の入力をユーザに要求する。

【0127】

図23は、図22の認証装置による登録処理のフローチャートである。まず、ID番号入力部151は、ユーザのID番号を入力する（ステップS171）。次のステップS172からS176までの処理については、図19のステップS131からS135までの処理と同様である。また、図23のステップS180からS183までの処理については、図19のステップS137からS140までの処理と同様である。ただし、ステップS183においては、生体特徴情報と補助情報を統合した登録データが作成される。

【0128】

ステップS176において登録データが作成されると、ID番号管理部162はID番号を保存し（ステップS177）、登録データ保存部164は登録データを保存し（ステップS178）、登録データ種類管理部161は登録データに含まれる生体特徴情報の種類を保存して（ステップS179）、処理を終了する。

【0129】

また、ステップS183において登録データが作成されると、ID番号管理部162はID番号を保存し（ステップS184）、登録データ保存部164は登録データを保存し（ステップS185）、登録データ種類管理部161は登録データに含まれる生体特徴情報と補助情報の種類を保存して（ステップS186）、処理を終了する。

【0130】

図24は、図22の認証装置による認証処理のフローチャートである。まず、ID番号入力部151は、ユーザのID番号を入力し（ステップS191）、登録データ種類管理部161は、生体情報入力部152と補助情報設定部155に入力データの種類を通知する（ステップS192）。

【0131】

次のステップS193からS198までの処理については、図20のステップS151からS156までの処理と同様である。また、次のステップS199からS201までの処理については、図5のステップS5からS7までの処理と同様である。また、ステップS202からS206までの処理については、図20のステップS158からS162までの処理と同様である。

【0132】

また、同一の照合方法に対応する複数個の生体特徴情報や、照合方法の異なる複数種類の生体特徴情報を登録データとして用いた場合にも、同様にして、ユーザのID番号毎に登録データの種類を登録しておくことができる。この場合、照合時に、入力されたID番号に対応する生体情報の入力が要求される。

【0133】

次に、クライアントからサーバに照合データを送信し、サーバで照合を行うクライアントサーバ型の認証システムについて説明する。このシステムでは、生体特徴情報をID番号と対応させて登録照合処理を行う場合に、補助情報の種類も登録しておく。照合時にクライアントからユーザのID番号が入力されると、そのID番号をもとにして、サーバ側から生体情報の入力を要求するとともに、所定の補助情報の入力も要求する。

【0134】

図25は、このような認証システムの構成図である。図25の認証システムは、クライアント171、サーバ172、およびそれらを接続するネットワークシステム173を備える。ネットワークシステム173は、LAN、WAN等の任意のネットワークを含む。

【0135】

クライアント171は、ID番号入力部181、生体情報入力部182、生体特徴情報抽出部183、照合精度推定部184、補助情報入力部185、照合データ作成部186、通信部187、および制御部188を備える。

【0136】

サーバ172は、ID番号対応データ検索部191、補助情報要求部192、通信部193、照合部194、照合結果判定部195、保存部196、および制御部197を備える。照合部194は、生体特徴情報照合部198、照合データ分離部199、および補助情報照合部200を含み、保存部196は、ID番号データベース(DB)201、登録データ種類DB202、生体特徴情報登録保存部203、および補助情報登録保存部204を含む。

【0137】

生体情報入力部182、生体特徴情報抽出部183、照合精度推定部184、補助情報入力部185、照合データ作成部186、通信部187、制御部188、通信部193、生体特徴情報照合部198、照合データ分離部199、補助情報照合部200、照合結果判定部195、生体特徴情報登録保存部203、補助情報登録保存部204、および制御部197の動作は、図14の認証システムの場合と同様である。

【0138】

照合データ作成部186と照合データ分離部199は、それぞれ、図22の登録データ作成部163と登録データ分離部165の役割も果たしている。また、ID番号入力部181、ID番号DB201、および登録データ種類DB202は、それぞれ、図22のID番号入力部151、ID番号管理部162、および登録データ種類管理部161に対応する。

【0139】

照合時に、ID番号入力部181がユーザの登録ID番号を入力すると、入力されたID番号はサーバ172に送られる。ID番号対応データ検索部191は、受け取ったID番号をキーとしてID番号DB201と登録データ種類DB202を検索し、ID番号に対応する登録データの種類を取得する。補助情報要求部192は、その登録データの種類を必要な照合データの種類としてクライアント171に通知し、補助情報入力部185は、通知された種類に対応する補助情報の入力をユーザに要求する。

【0140】

図26は、図25の認証システムによる登録処理のフローチャートである。図26のステップS211からS216までの処理については、クライアント171により行われ、図23のステップS171からS176までの処理と同様である。また、図26のステップS220からS223までの処理については、クライアント171により行われ、図23のステップS180からS183までの処理と同様である。

【0141】

ステップS216およびS223においては、照合データ作成部186が登録データを作成し、通信部187がそれをサーバ172に送信する。ステップS216において作成された登録データを通信部193が受信すると、ID番号DB201はID番号を保存し（ステップS217）、生体特徴情報登録保存部203は登録データに含まれる生体特徴情報を保存し（ステップS218）、登録データ種類DB202はその生体特徴情報の種類を保存して（ステップS219）、処理を終了する。

【0142】

また、ステップS223において作成された登録データを通信部193が受信すると、ID番号DB201はID番号を保存し（ステップS224）、生体特徴情報登録保存部203は登録データに含まれる生体特徴情報を保存し、補助情報登録保存部204は登録データに含まれる補助情報を保存し（ステップS225）、登録データ種類DB202は生体特徴情報と補助情報の種類を保存して（ステップS226）、処理を終了する。

【0143】

図27は、図25のクライアント171による認証処理のフローチャートである。まず、ID番号入力部151は、ユーザのID番号を入力し（ステップS231）、通信部187は、入力されたID番号をサーバ172に送信する（ステップS232）。サーバ172のID番号対応データ検索部191は、受信したID番号に対応する登録データの種類を取得し、補助情報要求部192は、それを照合用の入力データの種類としてクライアント171に送信する。

【0144】

通信部187は、入力データの種類を受信する（ステップS233）。次に、生体情報入力部182は、サーバ172からの通知に基づいて、照合用の生体情報の入力をユーザに要求し、生体情報を入力する（ステップS234）。また、補助情報入力部185は、サーバ172からの通知に基づいて、照合用の補助情報の入力をユーザに要求し、補助情報を入力する（ステップS235）。

【0145】

次に、生体特徴情報抽出部183は、生体情報から生体特徴情報を抽出し（ステップS236）、照合データ作成部186は、生体特徴情報と補助情報を結合して照合データを作成する。そして、通信部187は、作成された照合データをサーバ172に送信して（ステップS237）、処理を終了する。

【0146】

図28は、照合データを受信したサーバ172による認証処理のフローチャートである。図28のステップS241からS248までの処理は、照合データが生体特徴情報と補助情報に分解された後に行われ、図24のステップS199か

らS206までの処理と同様である。

【0147】

また、同一の照合方法に対応する複数個の生体特徴情報や、照合方法の異なる複数種類の生体特徴情報を照合データとして用いた場合にも、同様にして、クライアント側で登録データおよび照合データが作成され、サーバ側で登録と照合が行われる。

【0148】

図29は、クライアントサーバ型の認証システムで用いられる照合データの組合せを示している。図29において、クライアント211からサーバ212に送られる照合データ213は、生体特徴情報と補助情報を組み合わせたり、同一種類の複数個の生体特徴情報を組み合わせたり、複数種類の生体特徴情報を組み合わせたりして作成される。補助情報の例としてはパスワードが示され、複数個の生体特徴情報の例としては人指し指指紋特徴情報と中指指紋特徴情報が示されている。

【0149】

ところで、クライアントサーバ型の認証方法としては、リモート認証ダイヤルインユーザサービス (remote authentication dial-in user service, RADIUS) 形式のリモート認証や、ポイントツーポイントプロトコル (point to point protocol, PPP) 形式のダイヤルアップ認証が考えられる。

【0150】

RADIUS形式のリモート認証を用いた場合、クライアントで作成された登録データまたは照合データを、RADIUSプロトコルのユーザ名 (USER-NAME) 領域およびユーザパスワード (USER-PASSWORD) 領域に格納して、クライアントからサーバに送信する。また、登録データまたは照合データを、RADIUSプロトコルのEAP (extensible authentication protocol) メッセージ領域に格納して、クライアントからサーバに送信してもよい。

【0151】

このように、照合データを固まりとして扱い、RADIUSプロトコルの特定領域に格納して送信することで、RADUIS形式のリモート認証手順をそのまま

ま利用することができる。

【0152】

また、PPP形式のダイヤルアップ認証を用いた場合、クライアントで作成された登録データまたは照合データを、PPPプロトコルのユーザ名領域およびユーザパスワード領域に格納して、クライアントからサーバに送信する。このように、照合データを固まりとして扱い、PPPプロトコルの特定領域に格納して送信することで、PPP形式のダイヤルアップ認証手順をそのまま利用することができる。

【0153】

また、ダイヤルアップサーバ型の認証システムの場合、クライアントは、登録データおよび照合データをPPP形式で転送可能な所定値以内のデータ量で格納して、サーバに送信するようとする。この所定値としては、例えば、300バイトが用いられる。これにより、RADIUS形式のリモート認証手順やPPP形式のダイヤルアップ認証手順をそのまま利用することができる。

【0154】

また、図30に示すように、ユーザが入力するID番号に、登録データの種類に対応した識別コード（例えば、キャラクタコード）を付加しておいてもよい。このような識別コードを用いれば、クライアントは、ID番号が入力された時点で、どのような種類の生体情報もしくは補助情報の入力を要求すればよいかを、サーバへの問い合わせなしに判断することができる。

【0155】

また、図31に示すように、照合データ内に、生体情報および補助情報の種類を表す情報を記述しておいてもよい。このような種類情報を付加することで、照合データが照合部に送られた際に、照合データの分離を容易にすることができる。登録データについても同様である。

【0156】

また、図32に示すように、照合データ内に、照合データの構成を表すフォーマット情報を記述しておいてもよい。このようなフォーマット情報を付加することで、照合データが照合部に送られた際に、照合データの分離を容易にすること

ができる。登録データについても同様である。

【0157】

次に、第8の認証装置は、登録の際に、生体特徴情報と補助情報を登録し、照合時に、生体情報と補助情報の入力をユーザに求める。補助情報の入力を要求することで、生体情報が変動を受けた場合や生体特徴情報の再現性が悪い場合でも、所定の照合精度の照合結果が得られる。したがって、生体情報が使用不可能になることなく、本人確認が容易に行われる。

【0158】

図33は、このような認証装置の構成図である。図33の認証装置は、生体情報入力部221、生体特徴情報抽出部222、補助情報入力部223、照合部224、照合結果判定部225、保存部226、および制御部227を備える。照合部224は、生体特徴情報照合部228と補助情報照合部229を含み、保存部226は、生体特徴情報登録保存部230と補助情報登録保存部231を含む。各部の動作は図2の認証装置の場合と同様であるが、照合精度推定部と補助情報設定部がないので、よりシンプルな構成になっている。

【0159】

図34は、図33の認証装置による認証処理のフローチャートである。まず、生体情報入力部221は、ユーザの生体情報を入力し（ステップS251）、補助情報入力部223は、補助情報を入力し（ステップS252）、生体特徴情報抽出部222は、入力された生体情報から生体特徴情報を抽出する（ステップS253）。次のステップS254からS261までの処理は、図28のステップS241からS248までの処理と同様である。

【0160】

以上説明した認証装置、クライアント、およびサーバは、図35に示すような情報処理装置（コンピュータ）を用いて構成することができる。図35の情報処理装置は、CPU（中央処理装置）241、メモリ242、入力装置243、出力装置244、外部記憶装置245、媒体駆動装置246、およびネットワーク接続装置247を備え、それらはバス248により互いに接続されている。

【0161】

メモリ242は、例えば、ROM (read only memory)、RAM (random access memory) 等を含み、処理に用いられるプログラムとデータを格納する。CPU241は、メモリ242を利用してプログラムを実行することにより、必要な処理を行う。

【0162】

入力装置243は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ユーザからの指示や情報の入力に用いられる。出力装置244は、例えば、ディスプレイ、プリンタ、スピーカ等であり、ユーザへの問い合わせや処理結果の出力に用いられる。

【0163】

外部記憶装置245は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク (magneto-optical disk) 装置等である。情報処理装置は、この外部記憶装置245に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ242にロードして使用することができる。また、外部記憶装置245は、登録データ、登録データの種類、ID番号等を保存するデータベースとしても用いることができる。

【0164】

媒体駆動装置246は、可搬記録媒体249を駆動し、その記録内容にアクセスする。可搬記録媒体249としては、メモリカード、フロッピーディスク、CD-ROM (compact disk read only memory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。管理者は、この可搬記録媒体249に上述のプログラムとデータを格納しておき、情報処理装置は、必要に応じて、それらをメモリ242にロードして使用することができる。

【0165】

ネットワーク接続装置247は、任意のネットワーク（回線）を介して外部の装置と通信し、通信に伴うデータ変換を行う。また、情報処理装置は、必要に応じて、ネットワーク接続装置247を介して上述のプログラムとデータを外部の装置から受け取り、それらをメモリ242にロードして使用することができる。

【0166】

図36は、図35の情報処理装置にプログラムとデータを供給することができ
るコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体249や外
部のデータベース250に保存されたプログラムとデータは、メモリ242にロ
ードされる。そして、CPU241は、そのデータを用いてそのプログラムを実
行し、必要な処理を行う。

【0167】

【発明の効果】

本発明によれば、生体情報を用いた個人認証技術において、ユーザの生体特徴
情報の再現性が悪い場合でも、付加的な認証データを用いることで精度の高い処
理を行うことができる。したがって、生体特徴情報の再現性が悪いユーザでも、
認証システムを利用することができる。

【0168】

また、生体特徴情報と付加的な認証データを1つの照合データとして転送する
ことで、クライアントサーバ型の認証システムにおける通信コストが削減される

【図面の簡単な説明】

【図1】

本発明の認証装置の原理図である。

【図2】

第1の認証装置の構成図である。

【図3】

生体特徴情報照合スコアの設定値を示す図である。

【図4】

補助情報照合スコアの設定値を示す図である。

【図5】

第1の認証処理のフローチャートである。

【図6】

第2の認証装置の構成図である。

【図7】

第2の認証処理のフローチャートである。

【図8】

第3の認証装置の構成図である。

【図9】

第3の認証処理のフローチャートである。

【図10】

第4の認証装置の構成図である。

【図11】

第4の認証処理のフローチャートである。

【図12】

第1の照合データを示す図である。

【図13】

照合データ作成処理のフローチャートである。

【図14】

第1のクライアントサーバシステムの構成図である。

【図15】

第1のクライアントの処理のフローチャートである。

【図16】

第1のサーバの処理のフローチャートである。

【図17】

第2のサーバの処理のフローチャートである。

【図18】

第5の認証装置の構成図である。

【図19】

第1の登録処理のフローチャートである。

【図20】

第5の認証処理のフローチャートである。

【図21】

第6の認証装置の構成図である。

【図22】

第7の認証装置の構成図である。

【図23】

第2の登録処理のフローチャートである。

【図24】

第6の認証処理のフローチャートである。

【図25】

第2のクライアントサーバシステムの構成図である。

【図26】

第3の登録処理のフローチャートである。

【図27】

第2のクライアントの処理のフローチャートである。

【図28】

第3のサーバの処理のフローチャートである。

【図29】

照合データの組み合わせを示す図である。

【図30】

ID番号を示す図である。

【図31】

第2の照合データを示す図である。

【図32】

第3の照合データを示す図である。

【図33】

第8の認証装置の構成図である。

【図34】

第7の認証処理のフローチャートである。

【図35】

情報処理装置の構成図である。

【図36】

記録媒体を示す図である。

【符号の説明】

- 1 生体情報入力手段
- 2 抽出手段
- 3 推定手段
- 4 要求手段
- 5 認証情報入力手段
- 6 生体特徴情報登録手段
- 7 認証情報登録手段
- 8 生体特徴情報照合手段
- 9 認証情報照合手段
- 10 判定手段

11、31、61、65、91、111、131、152、182、221

生体情報入力部

12、32、62、66、92、112、132、153、183、222

生体特徴情報抽出部

13、33、53、63、93、113、133、154、184 照合精度

推定部

14、94、114、134、155 助情報設定部

15、95、115、135、156、185、223 助情報入力部

16、37、54、67、102、117、137、158、194、224

照合部

17、38、55、68、103、118、138、159、195、225

照合結果判定部

18、39、56、69、104、116、136、157、196、226

保存部

19、40、57、70、98、105、119、139、160、188、

197、227 制御部

20、41、71、72、106、122、143、166、198、228

生体特徴情報照合部

21、108、123、144、167、200、229 補助情報照合部

22、43、73、74、109、120、203、230 生体特徴情報登
録保存部

23、110、121、204、231 補助情報登録保存部

34 パスワード情報設定部

35 パスワード桁数設定部

36 パスワード情報入力部

42 パスワード情報照合部

44 パスワード情報登録保存部

51 指紋情報入力部

52 指紋特徴情報抽出部

58 指紋特徴情報照合部

59 指紋特徴情報登録保存部

64 生体情報設定部

81、171、211 クライアント

82、172、212 サーバ

83、173 ネットワークシステム

96、186 照合データ作成部

97、101、187、193 通信部

107、199 照合データ分離部

140、163 登録データ作成部

141、164 登録データ保存部

142、165 登録データ分離部

151、181 ID番号入力部

161 登録データ種類管理部

162 ID番号管理部

191 ID番号対応データ検索部

192 補助情報要求部

- 201 ID番号データベース
- 202 登録データ種類データベース
- 213 照合データ
- 241 CPU
- 242 メモリ
- 243 入力装置
- 244 出力装置
- 245 外部記憶装置
- 246 媒体駆動装置
- 247 ネットワーク接続装置
- 248 バス
- 249 可搬記録媒体
- 250 データベース

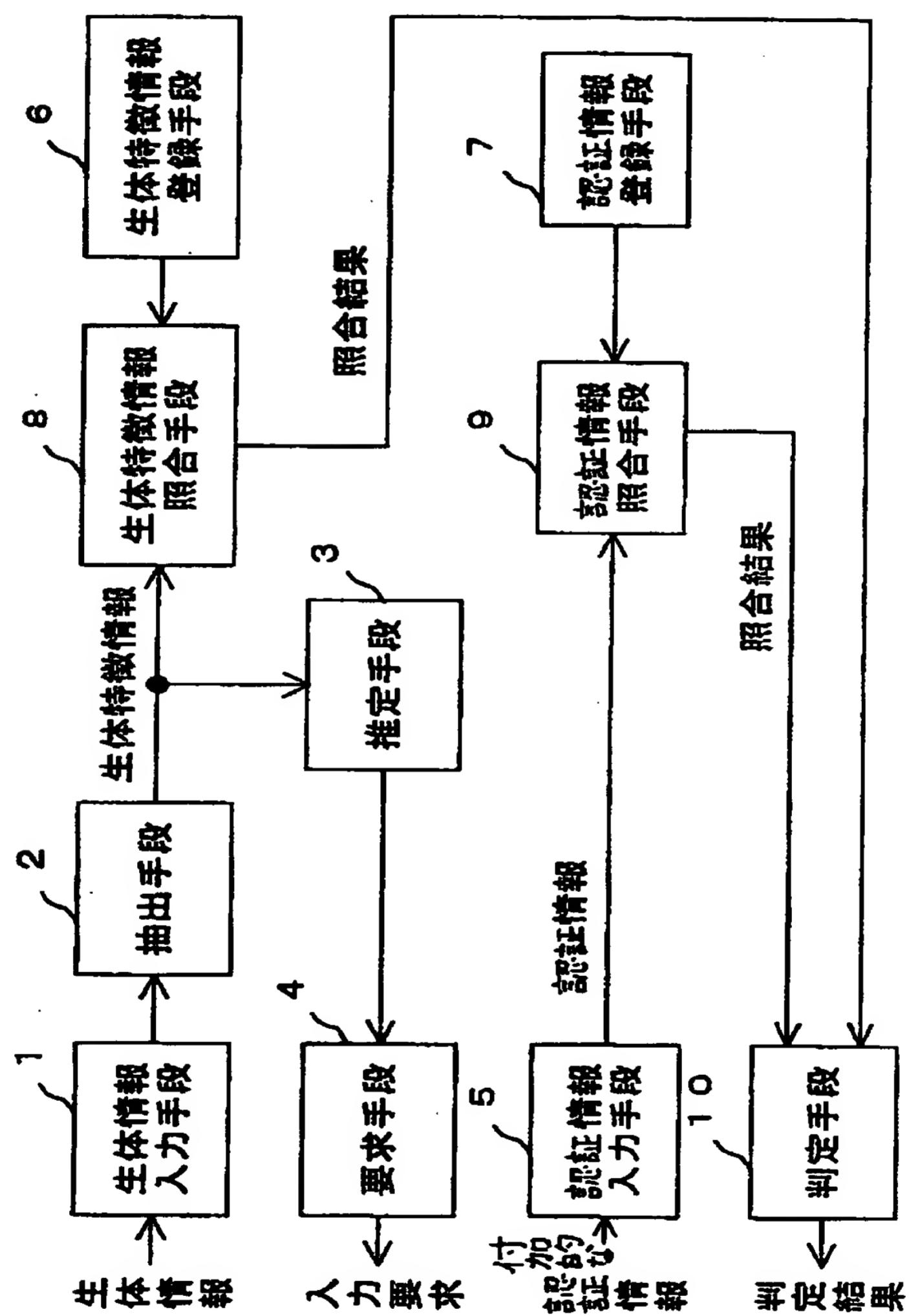
//

【書類名】

圖面

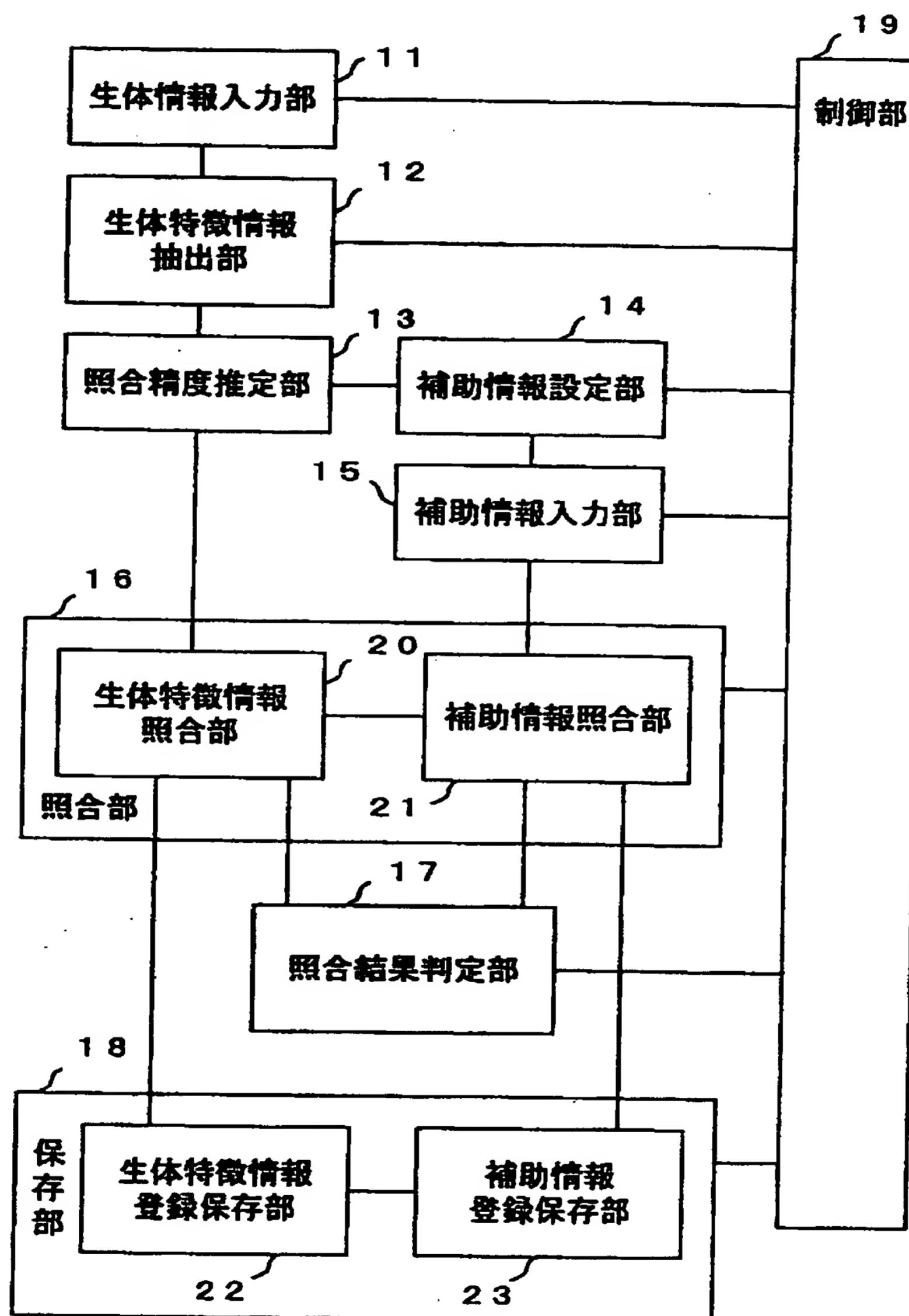
【図1】

本発明の原理説明図



【図2】

第1の認証装置の構成図



【図3】

生体特徴情報照合スコアの
設定値を示す図

照合スコア	1	2	3	4	5	6
他人受入率	1/1000000	1/100000	1/10000	1/1000	1/100	1/10

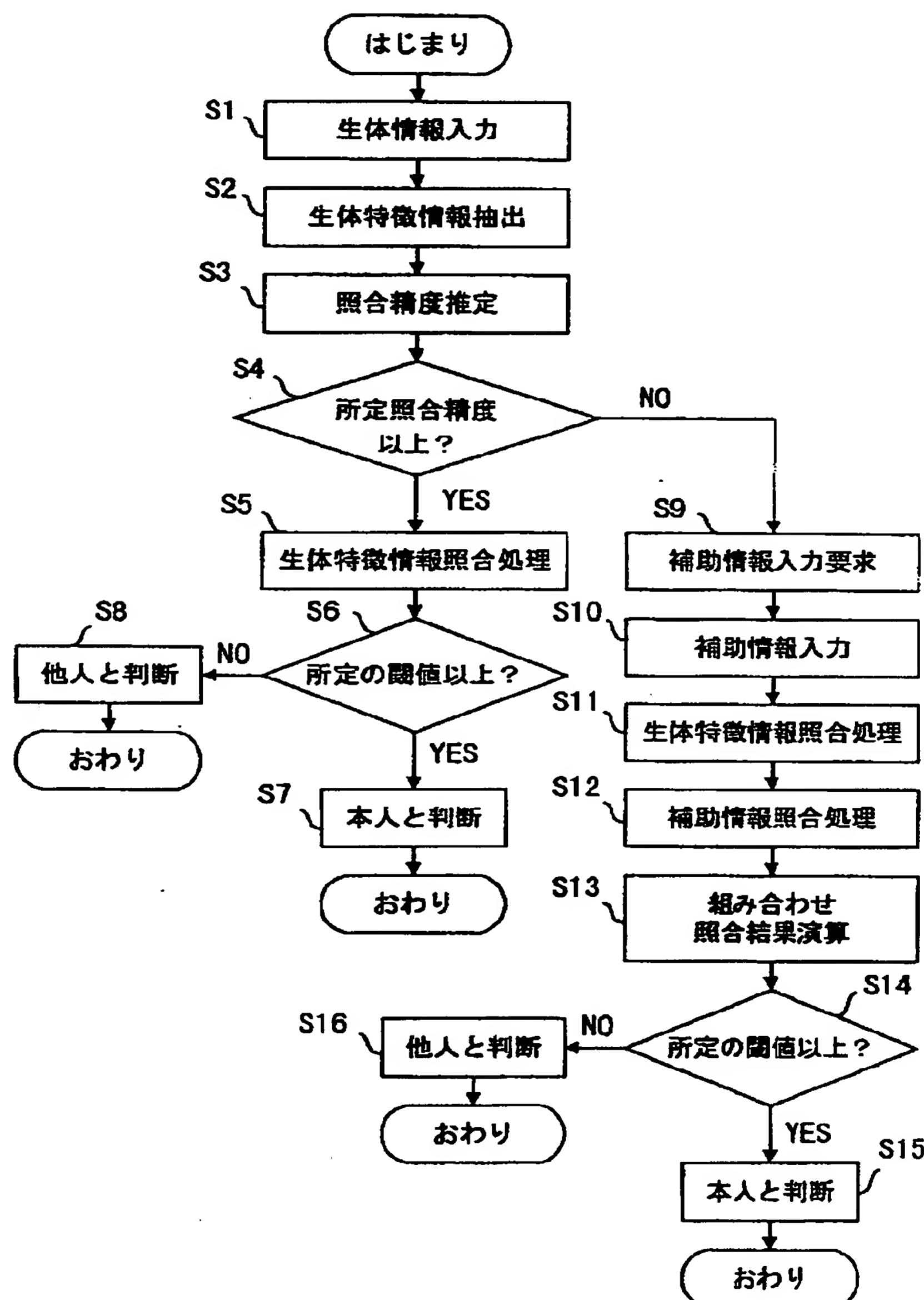
【図4】

補助情報照合スコアの
設定値を示す図

照合スコア	1 1	1 2	1 3	1 4	1 5
他人受入率	1/100000	1/10000	1/1000	1/100	1/10

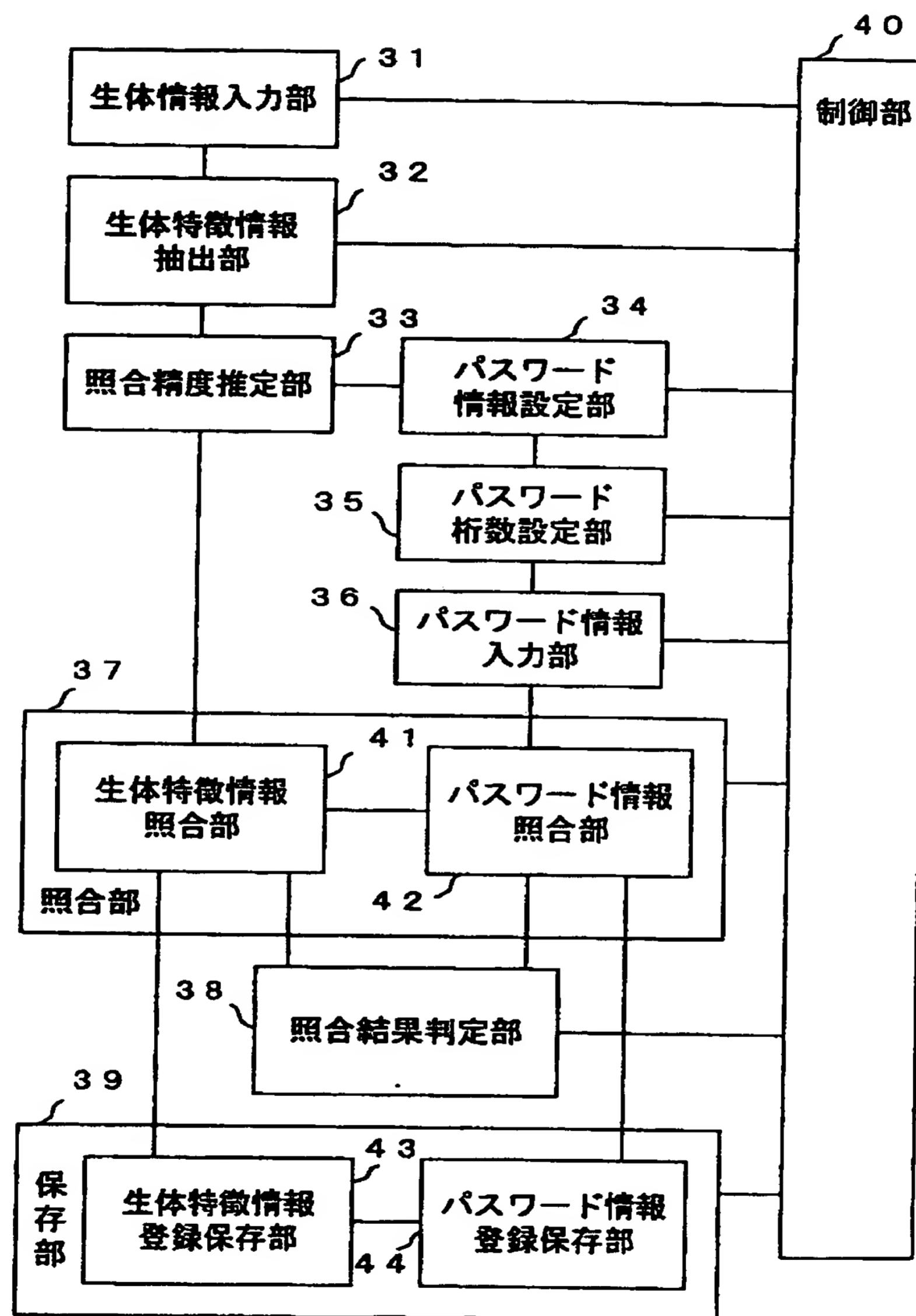
【図5】

第1の認証処理のフローチャート



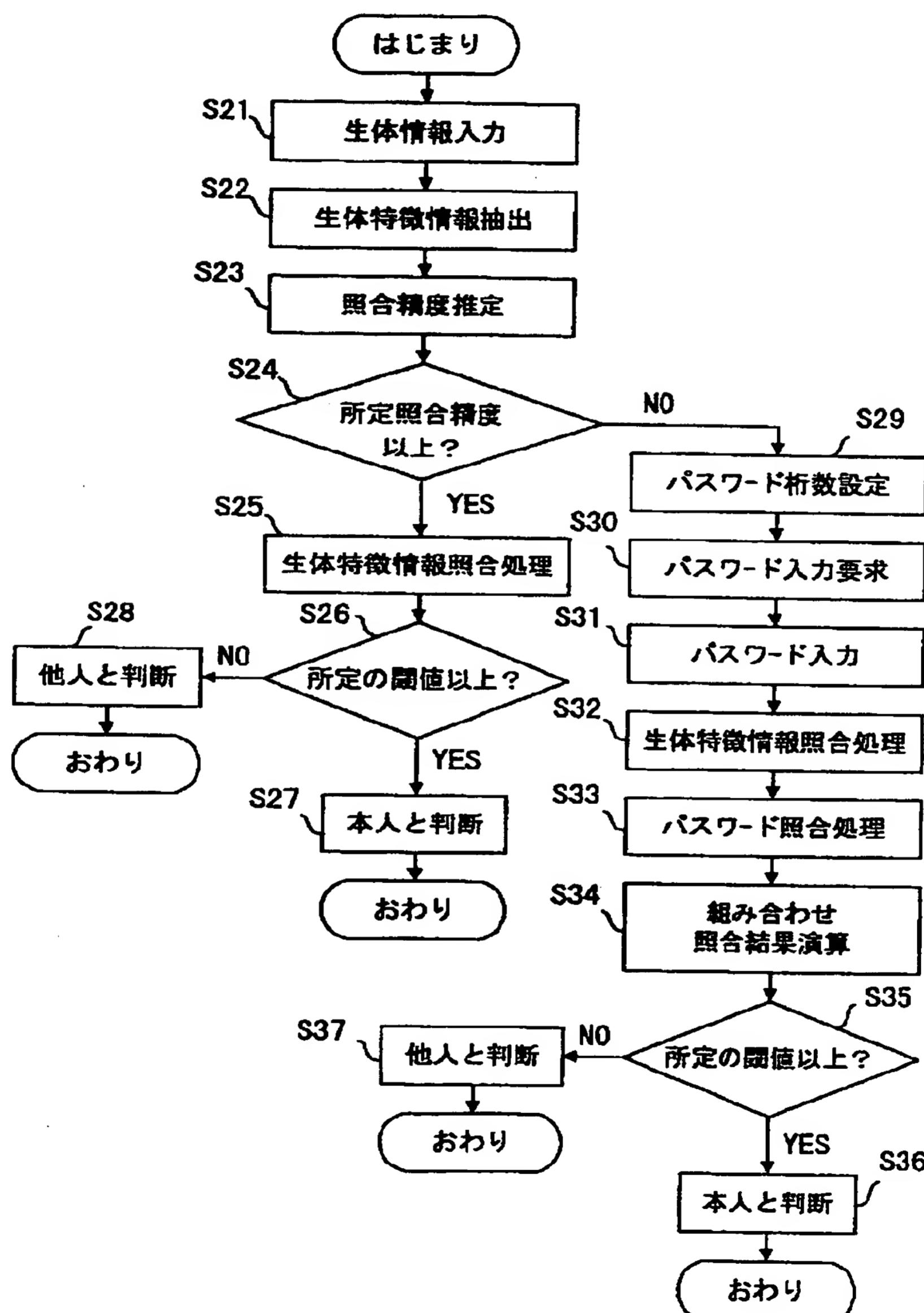
【図6】

第2の認証装置の構成図



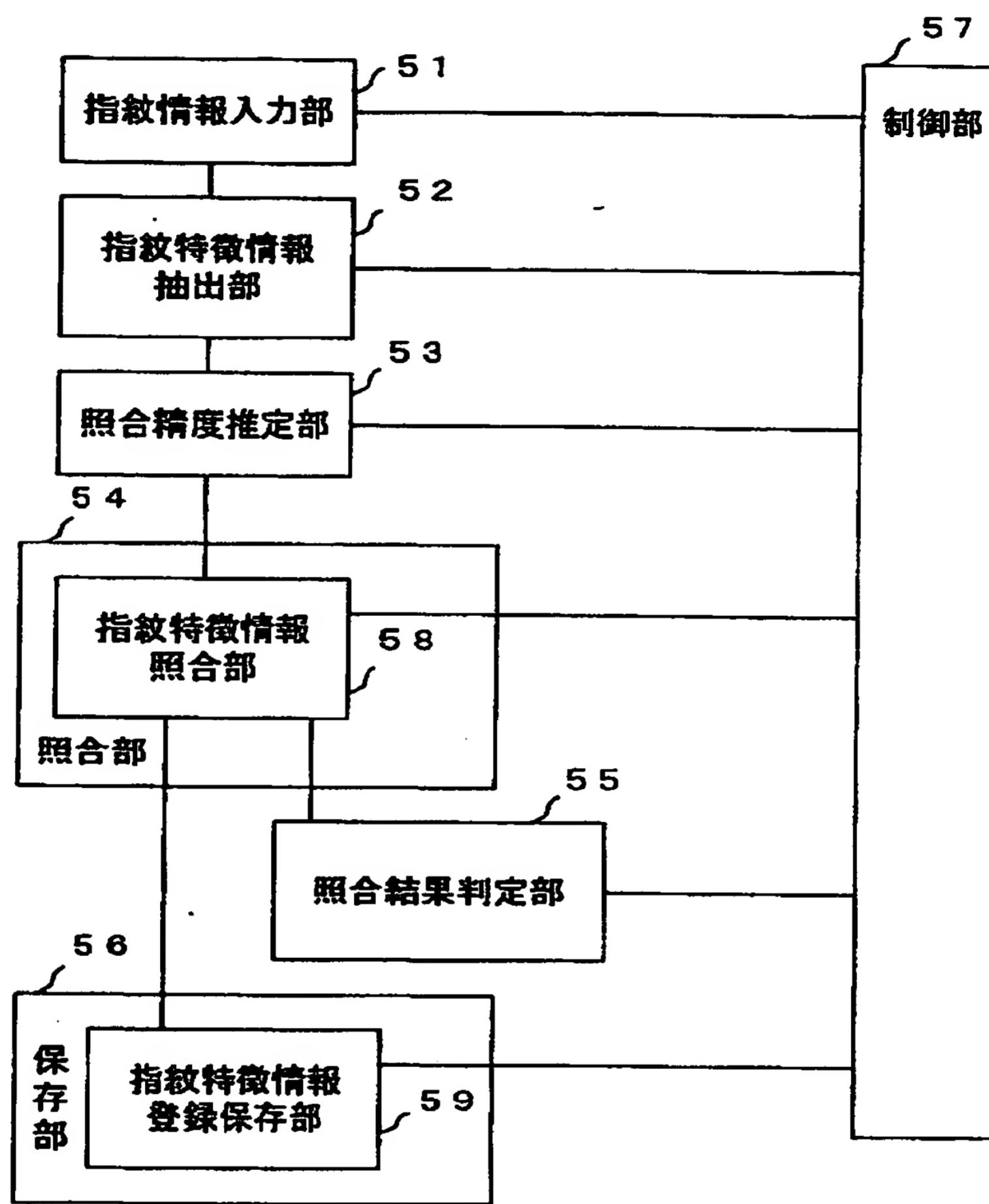
【図7】

第2の認証処理のフローチャート



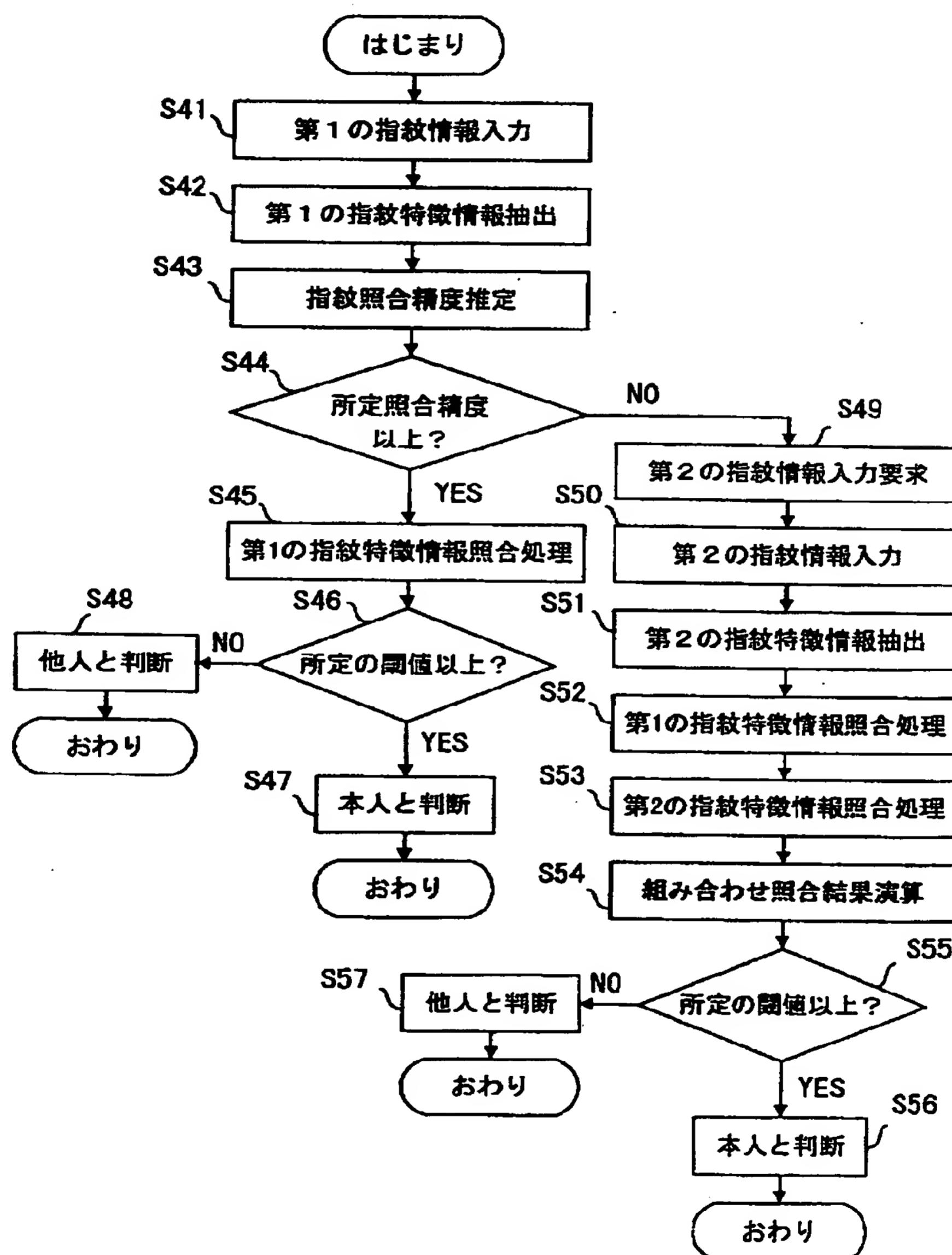
【図8】

第3の認証装置の構成図



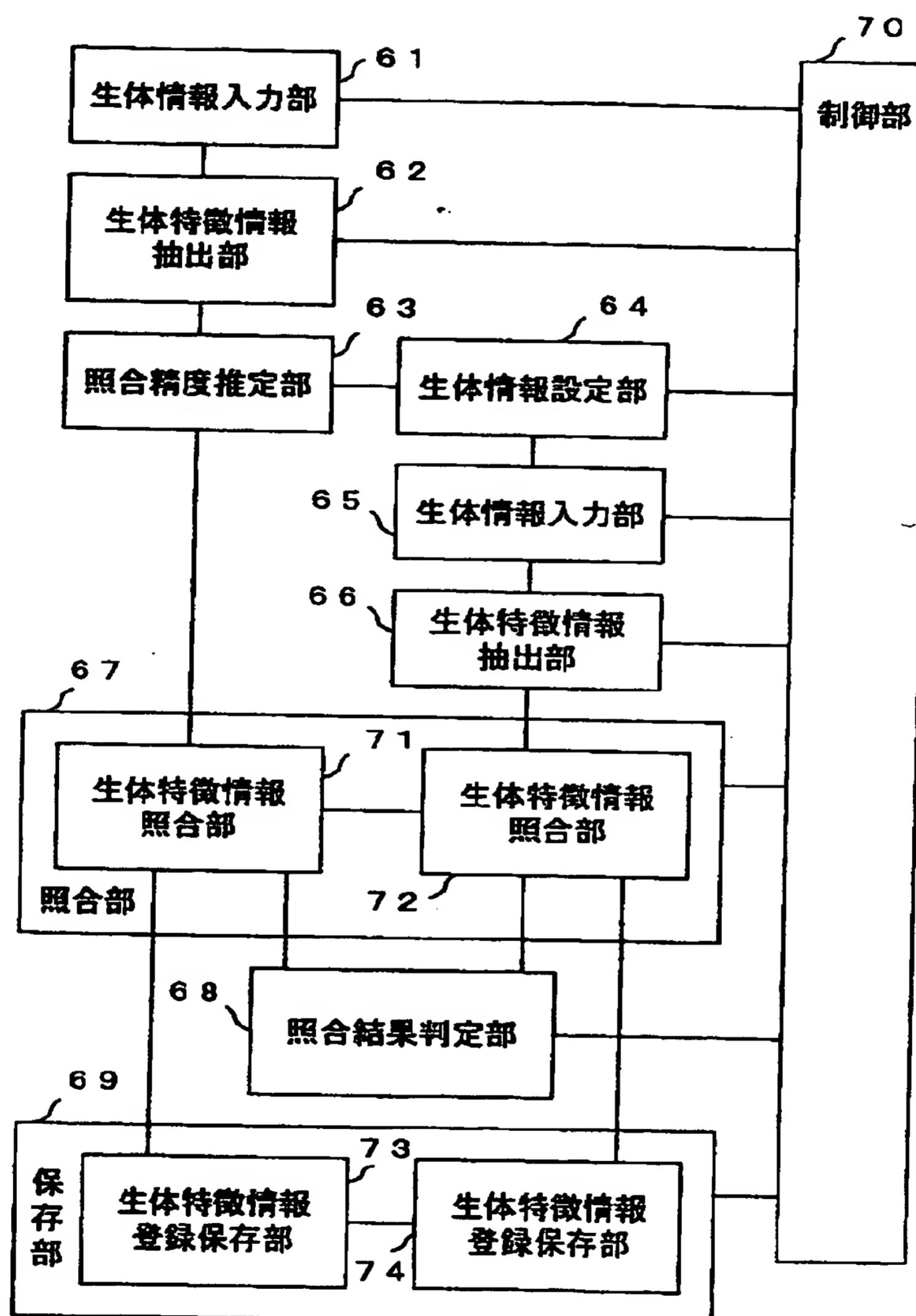
【図9】

第3の認証処理のフローチャート



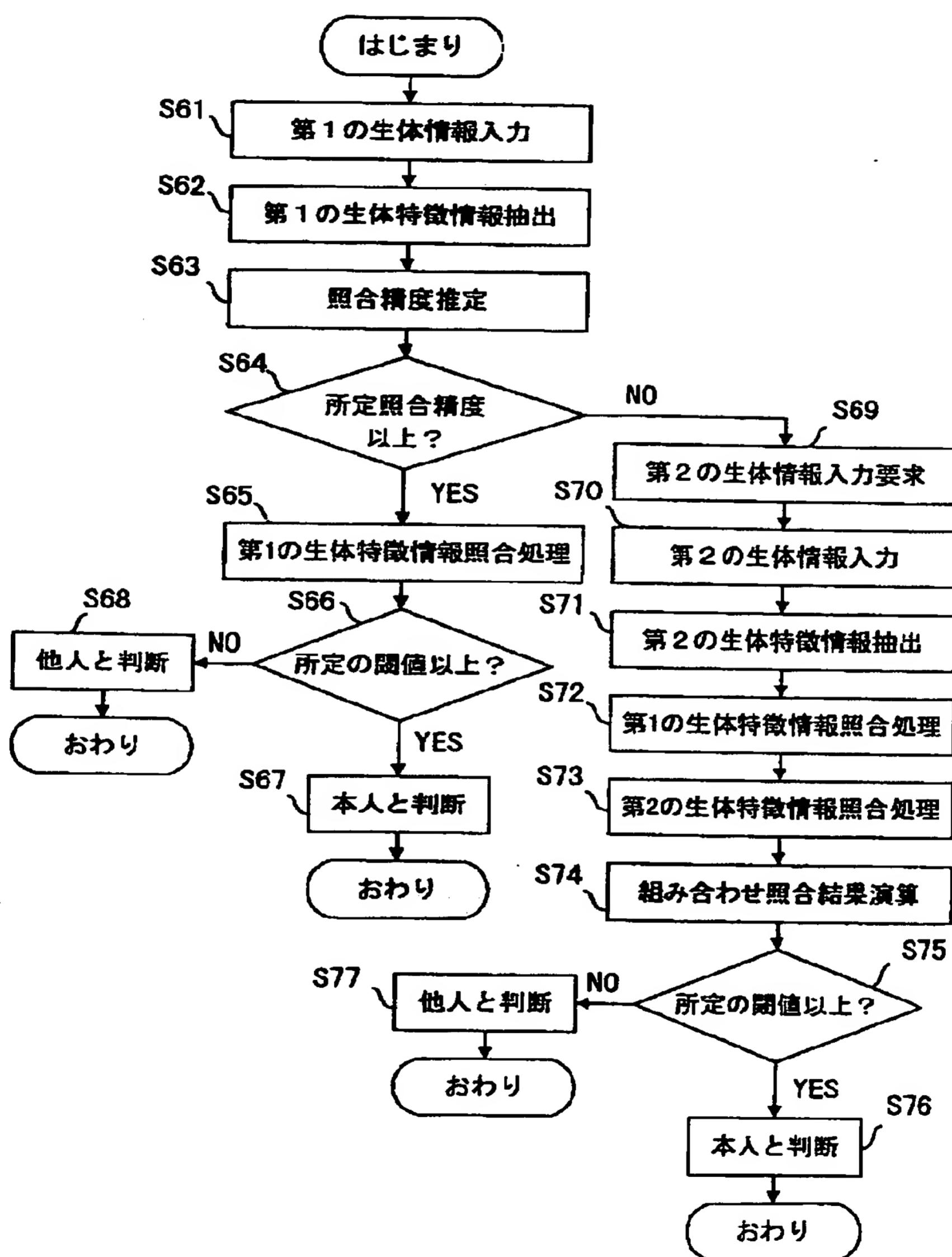
【図10】

第4の認証装置の構成図



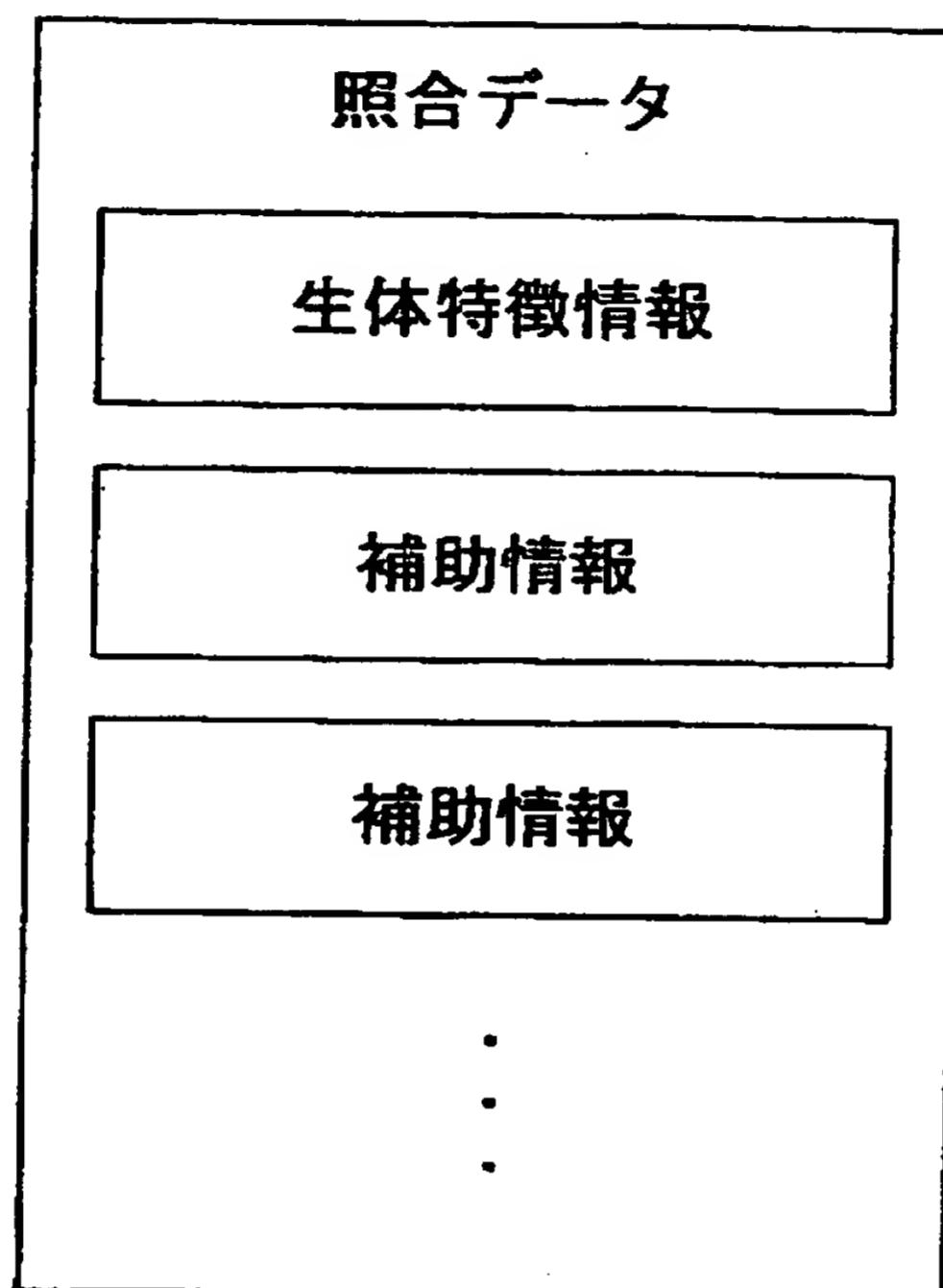
【図11】

第4の認証処理のフローチャート



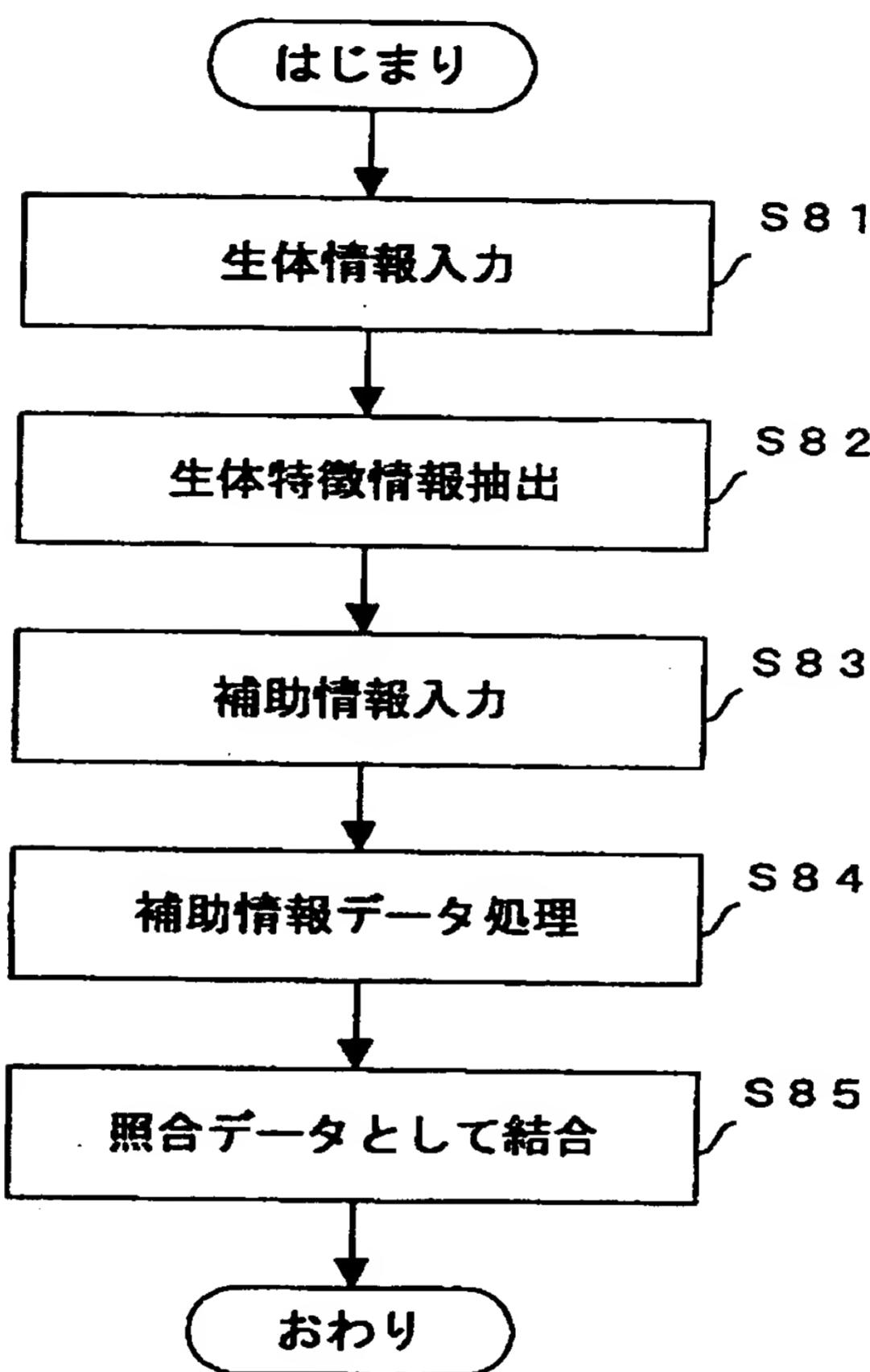
【図12】

第1の照合データを示す図



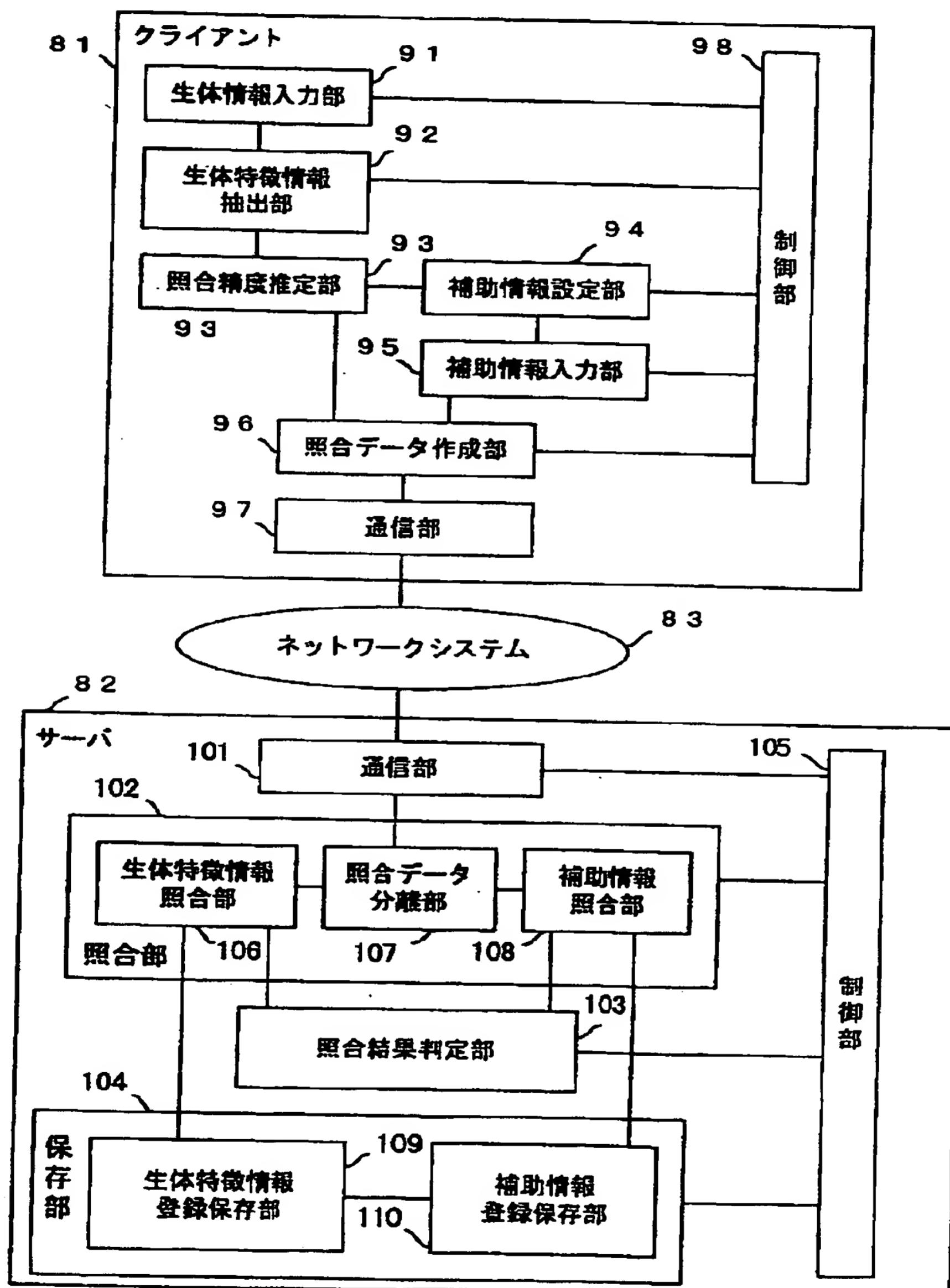
【図13】

照合データ作成処理の フローチャート



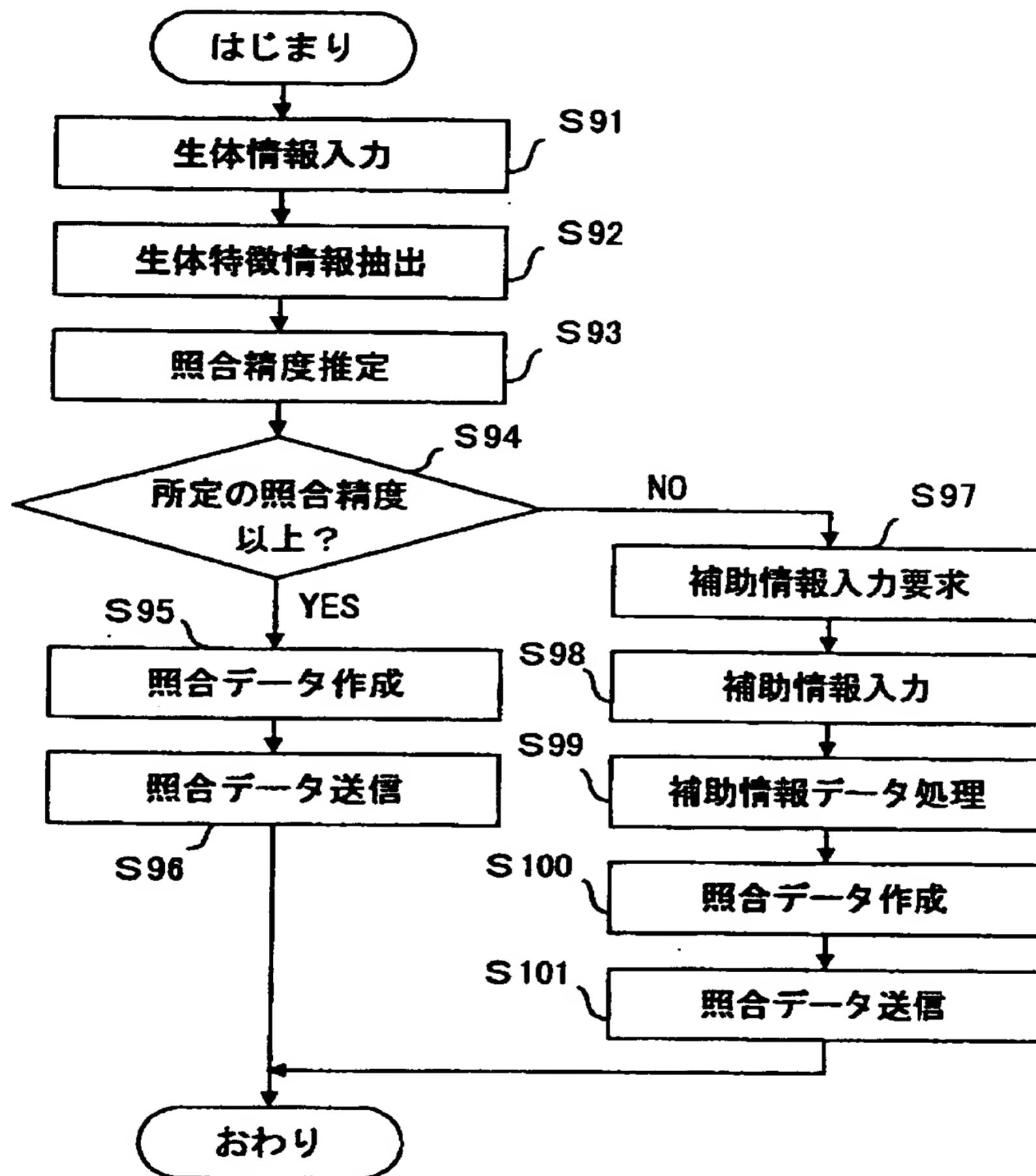
【図14】

第1のクライアントサーバシステムの構成図



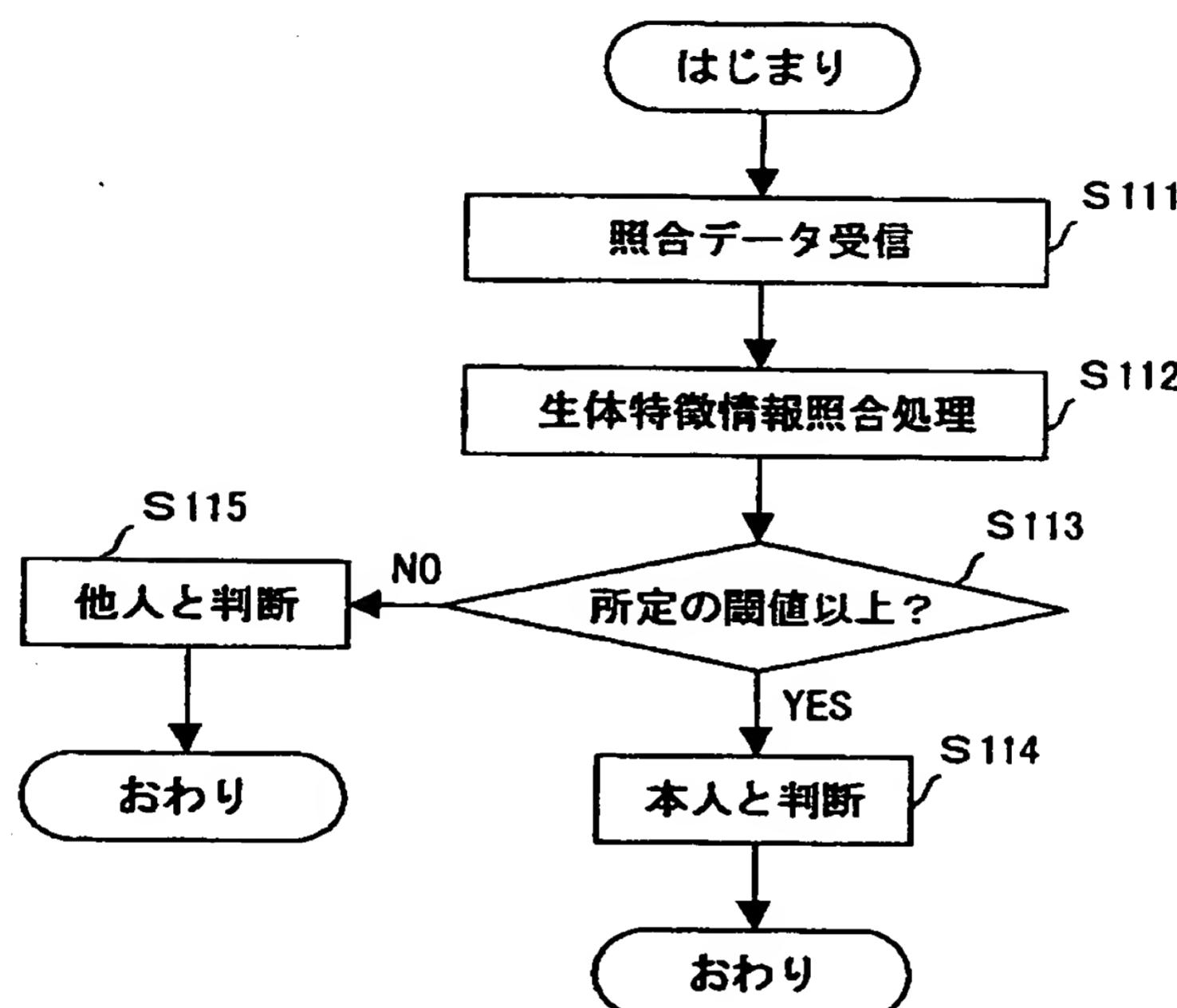
【図15】

第1のクライアントの処理のフローチャート



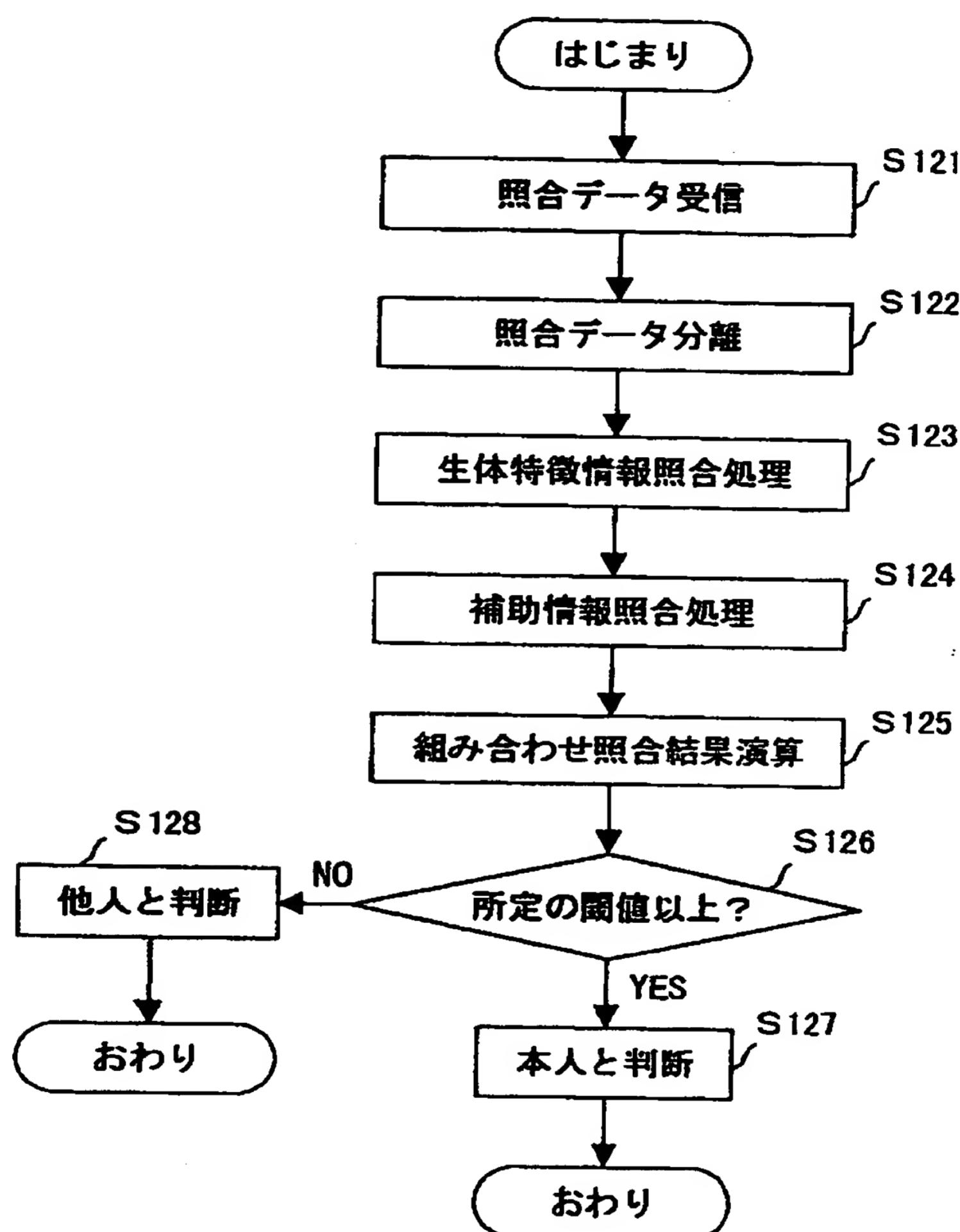
【図16】

第1のサーバの処理のフローチャート



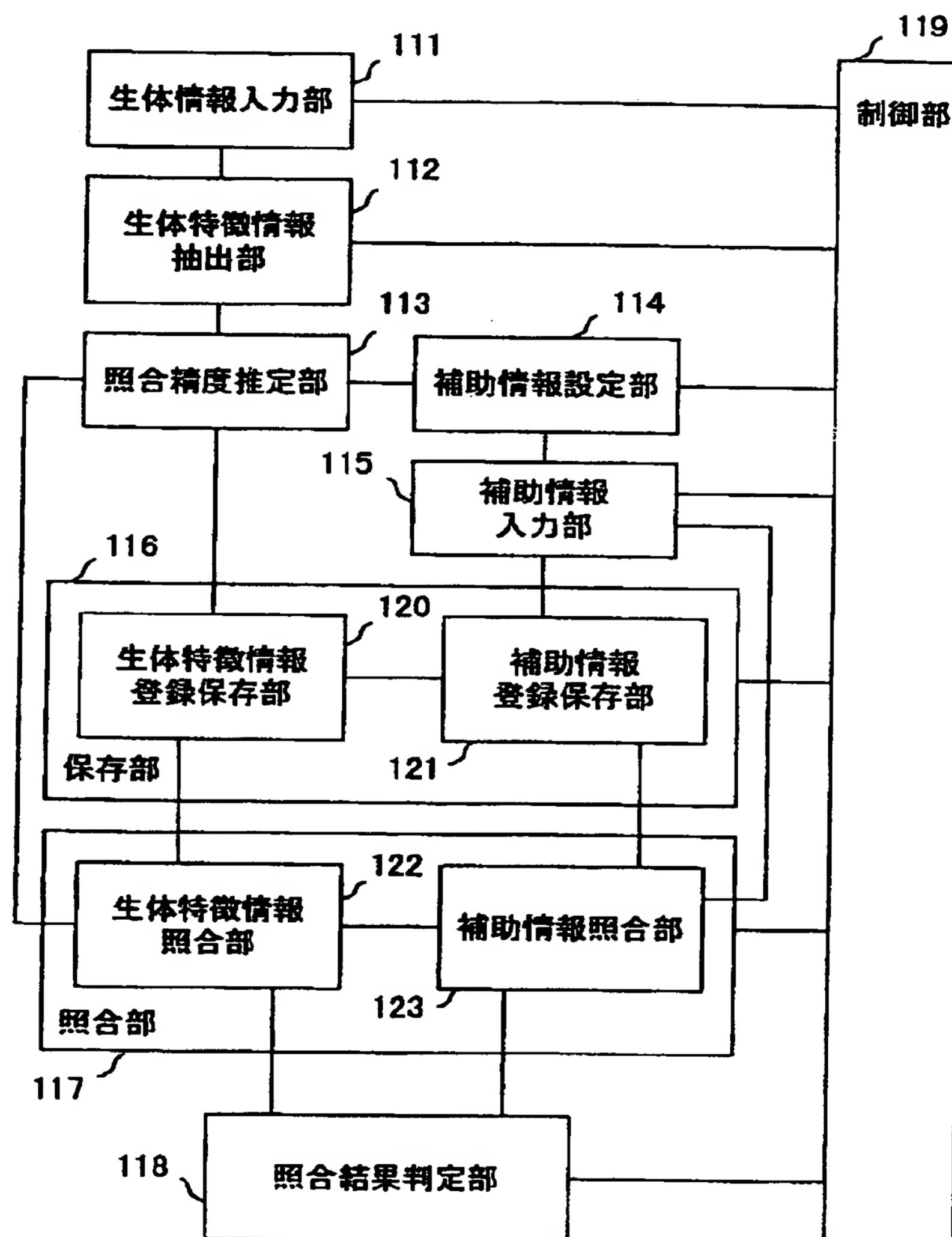
【図17】

第2のサーバの処理のフローチャート



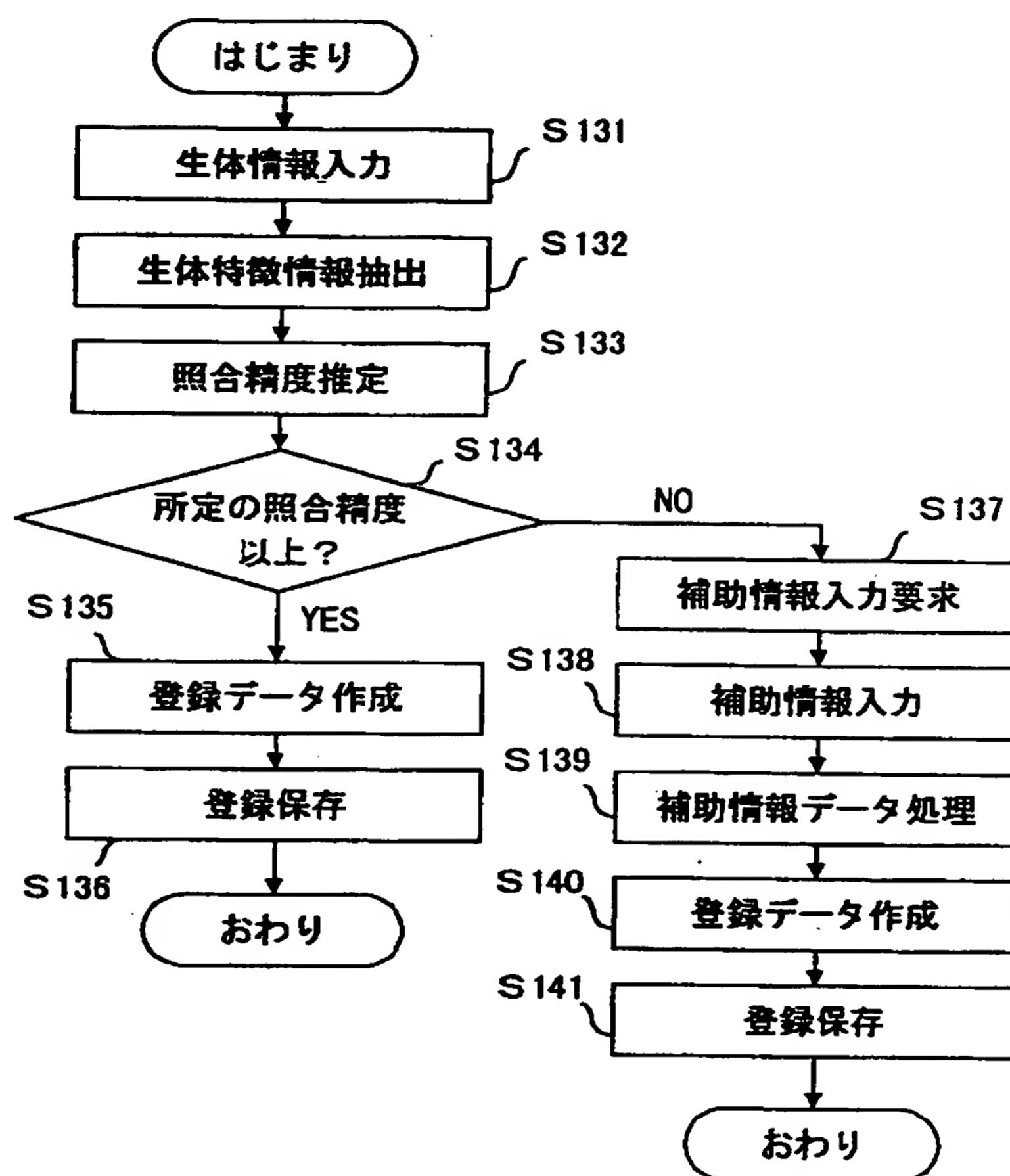
【図18】

第5の認証装置の構成図



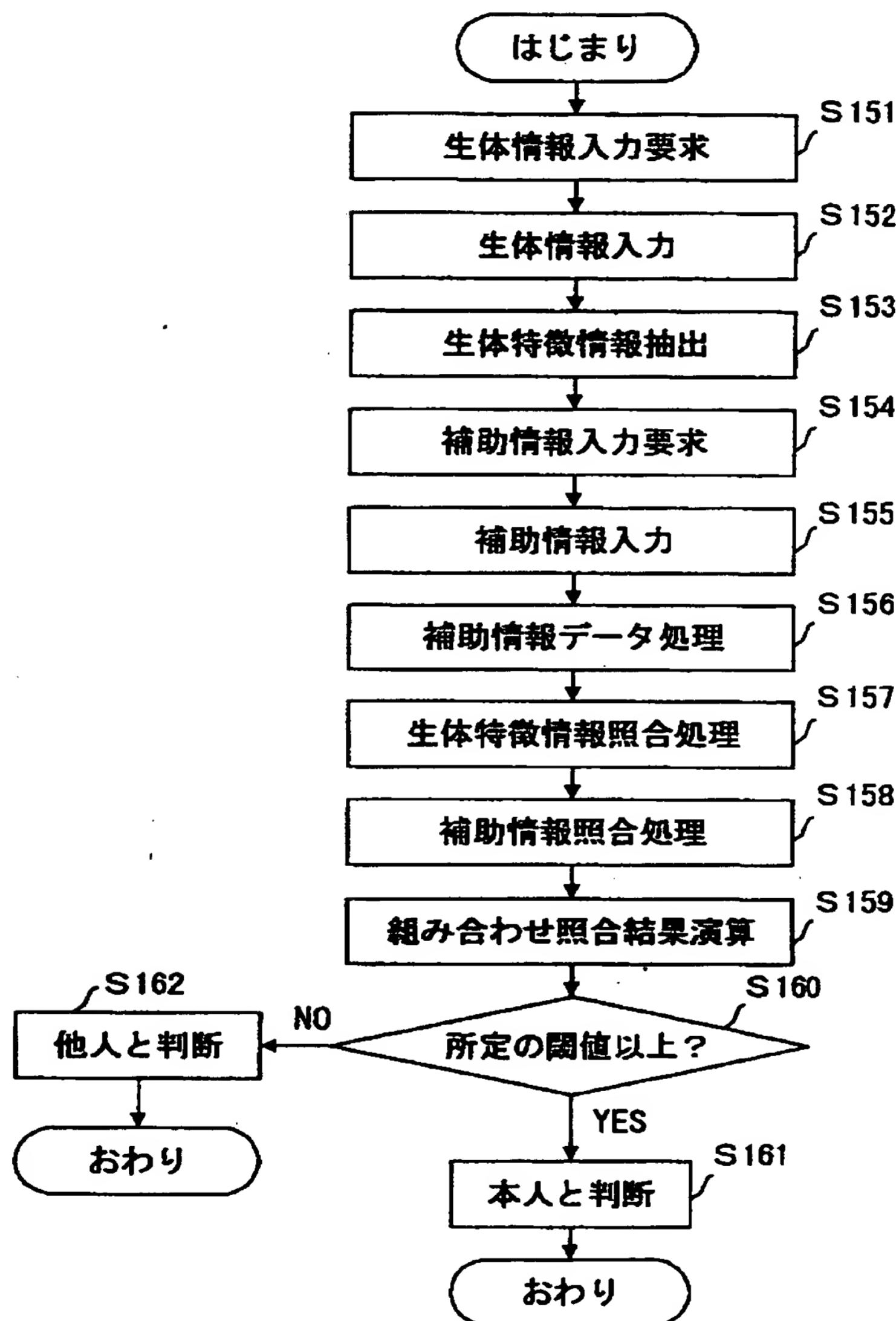
【図19】

第1の登録処理のフローチャート



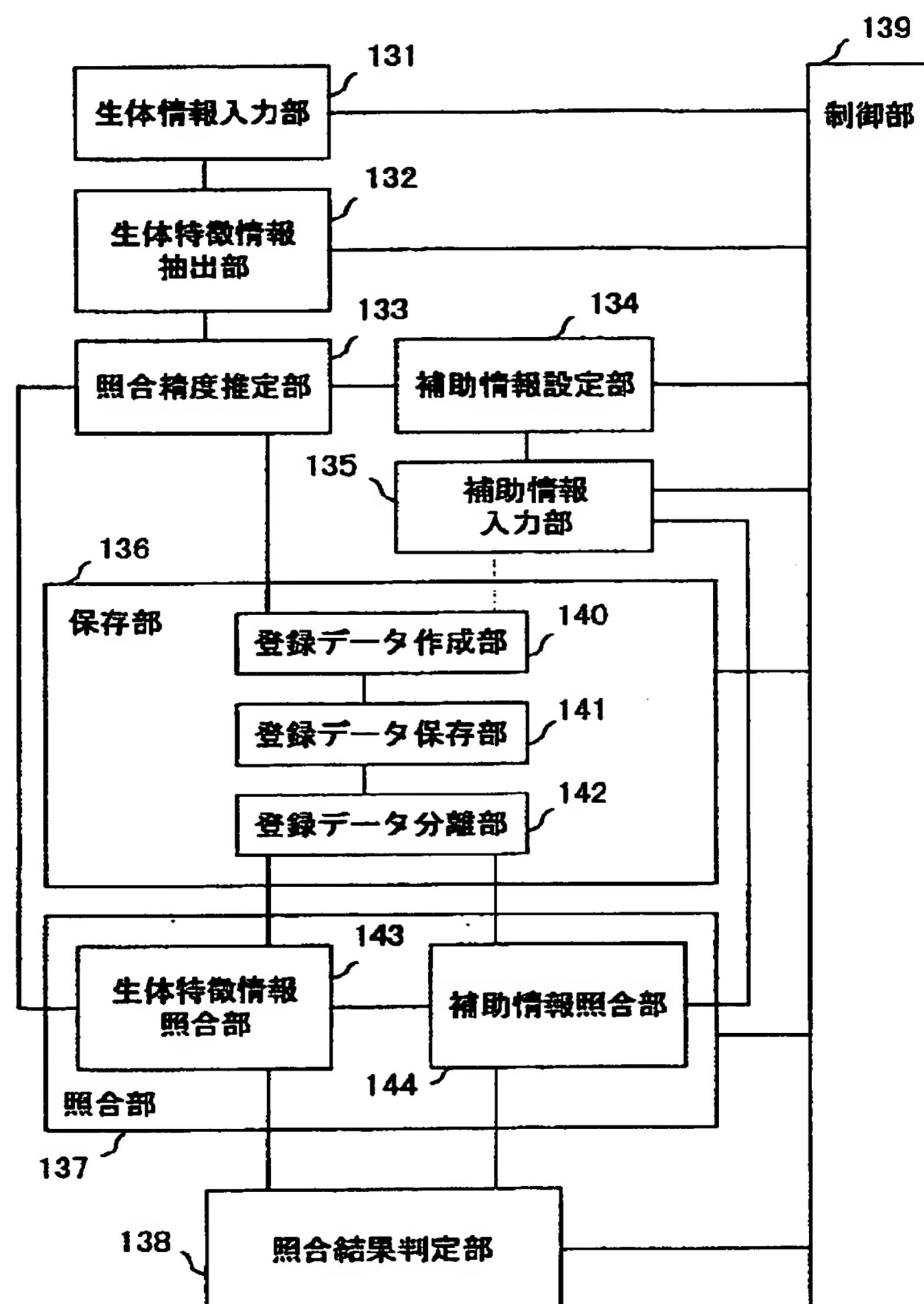
【図20】

第5の認証処理のフローチャート



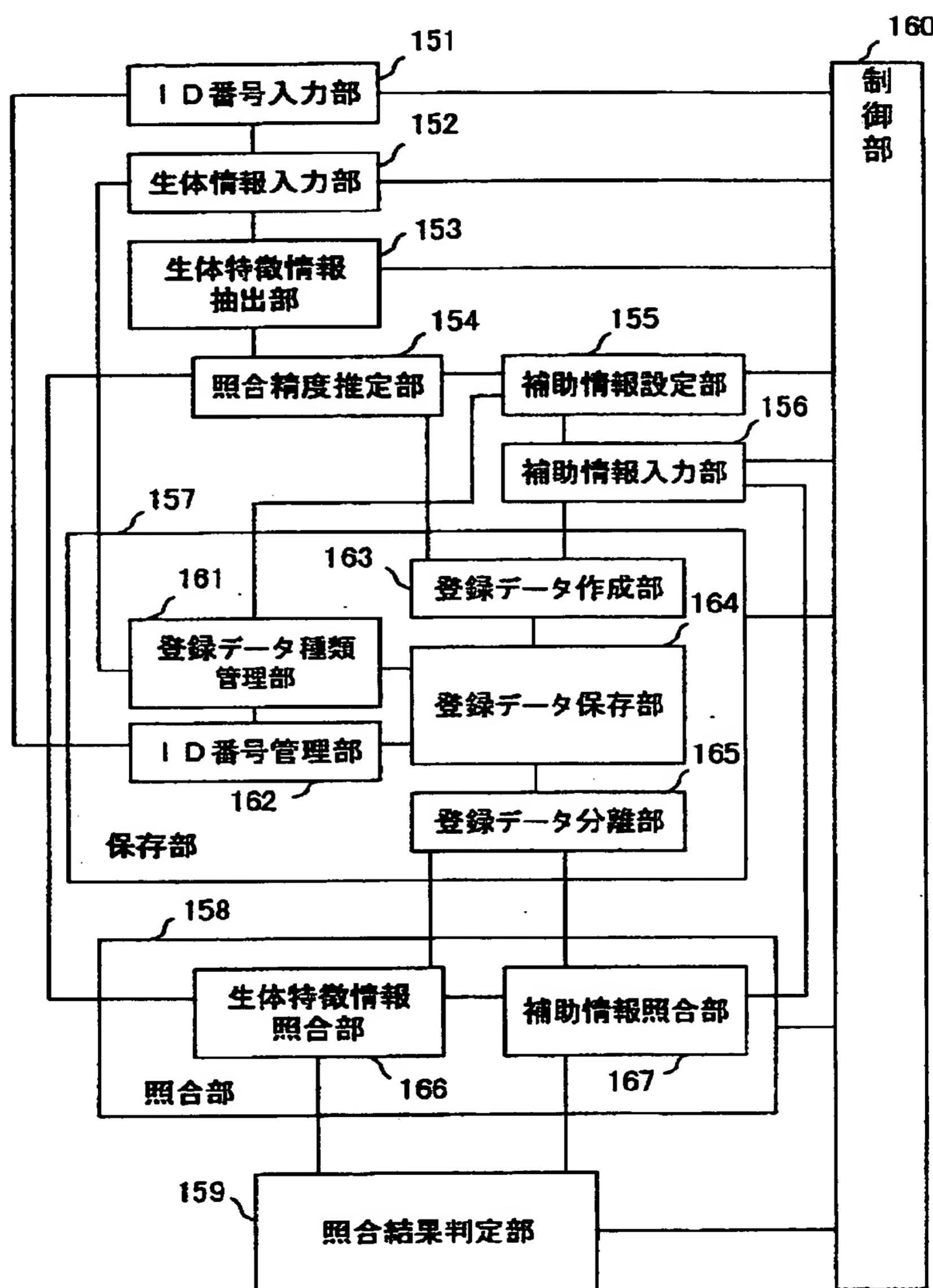
【図21】

第6の認証装置の構成図



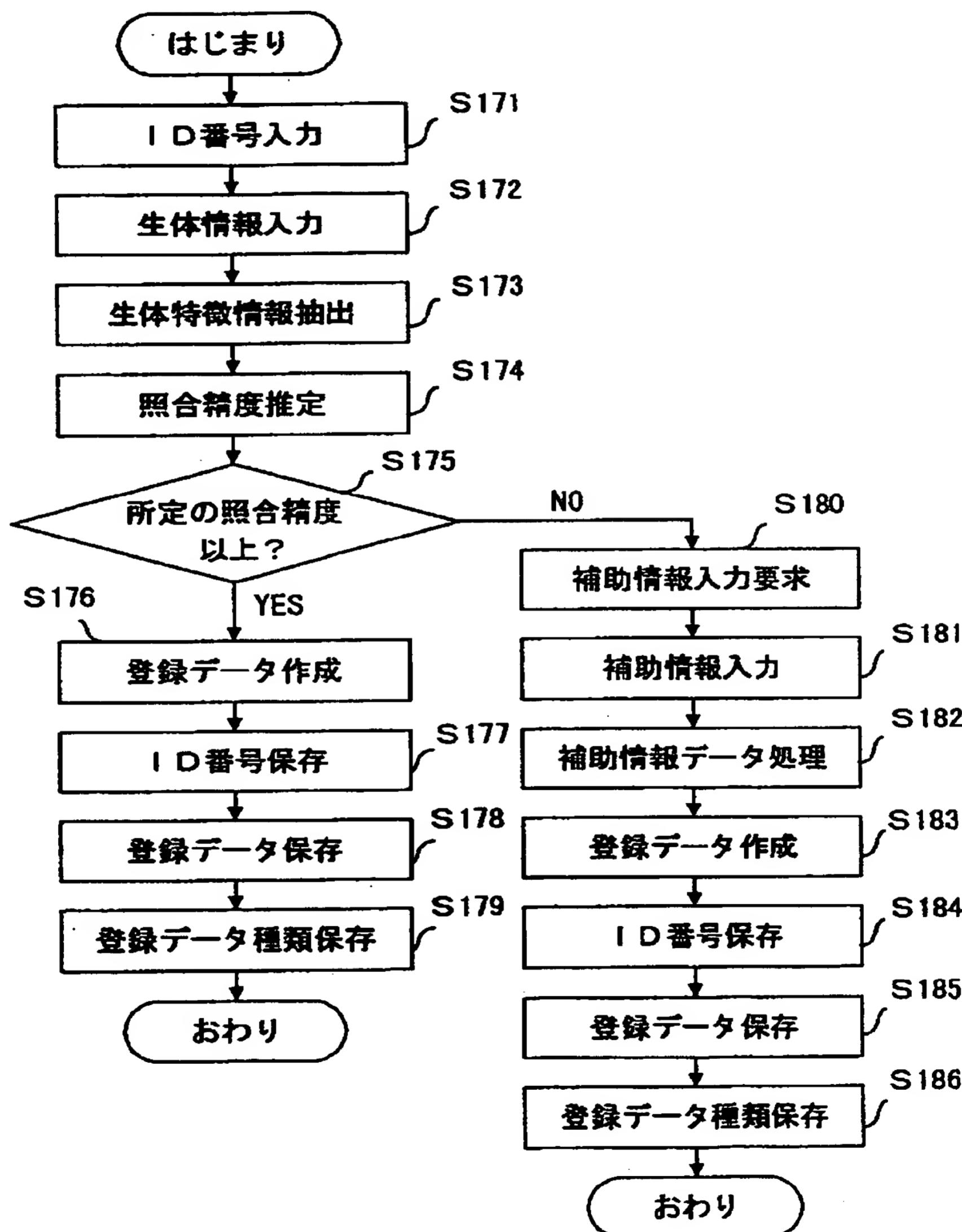
【図22】

第7の認証装置の構成図



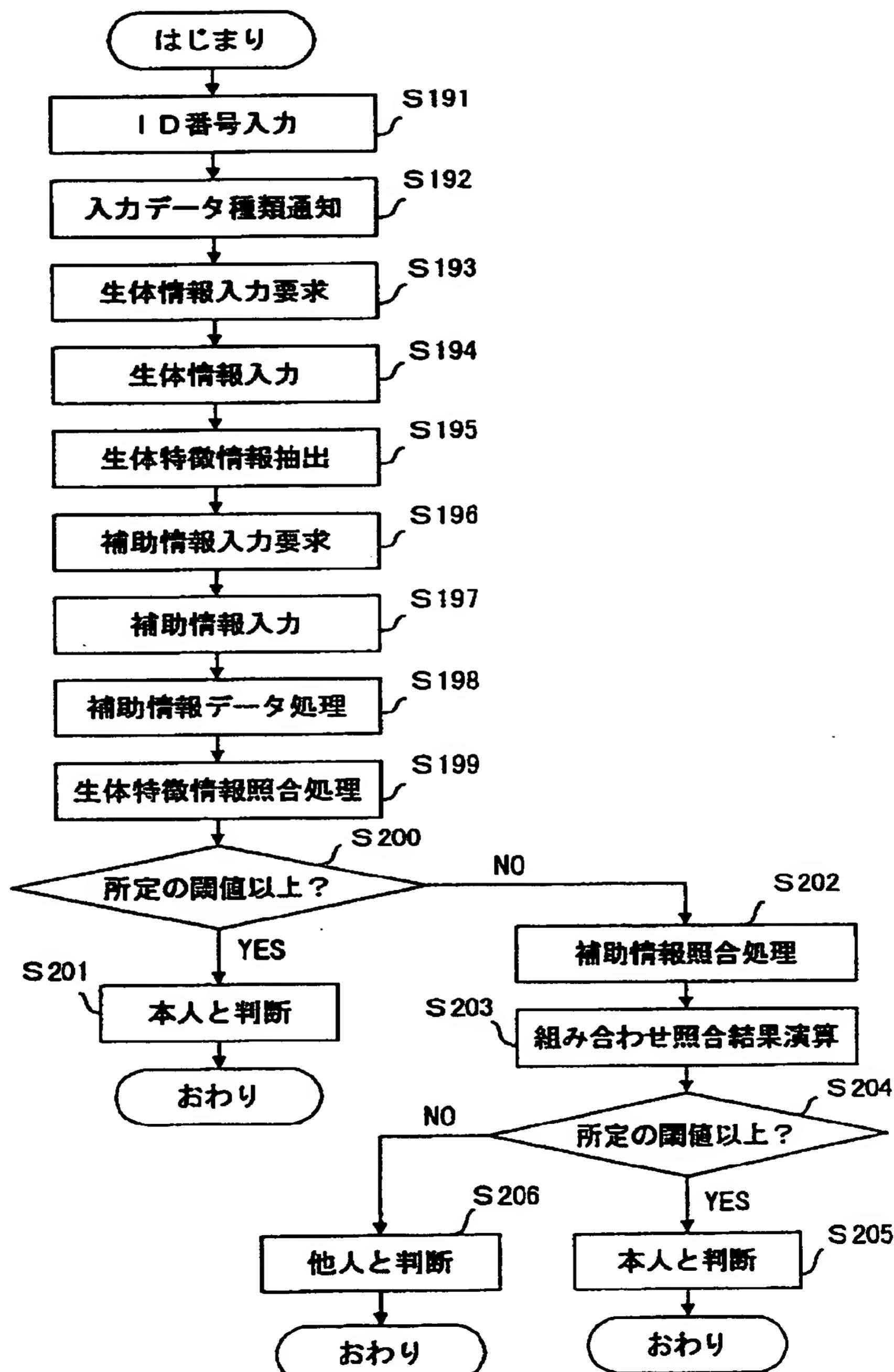
【図23】

第2の登録処理のフローチャート



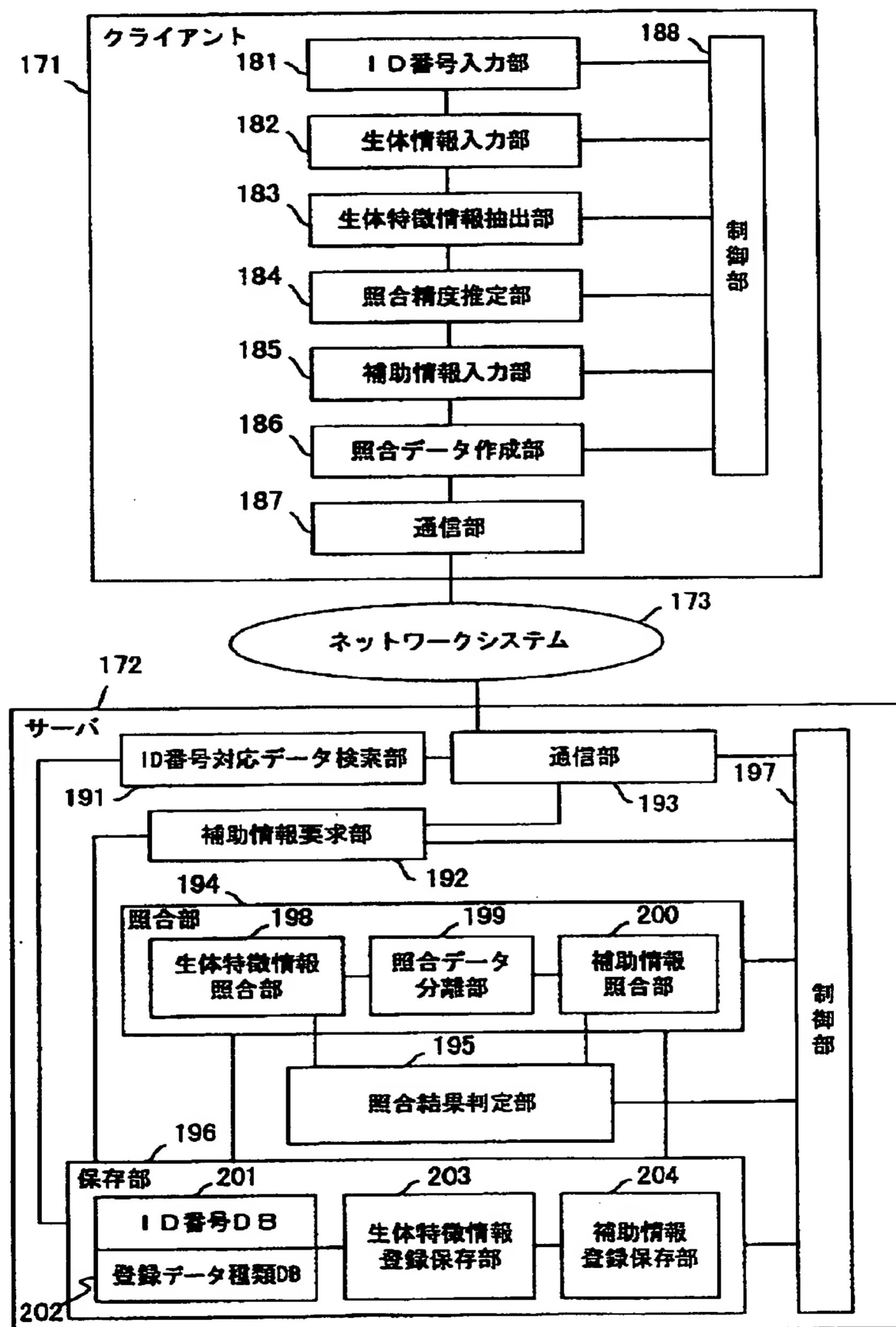
【図24】

第6の認証処理のフローチャート



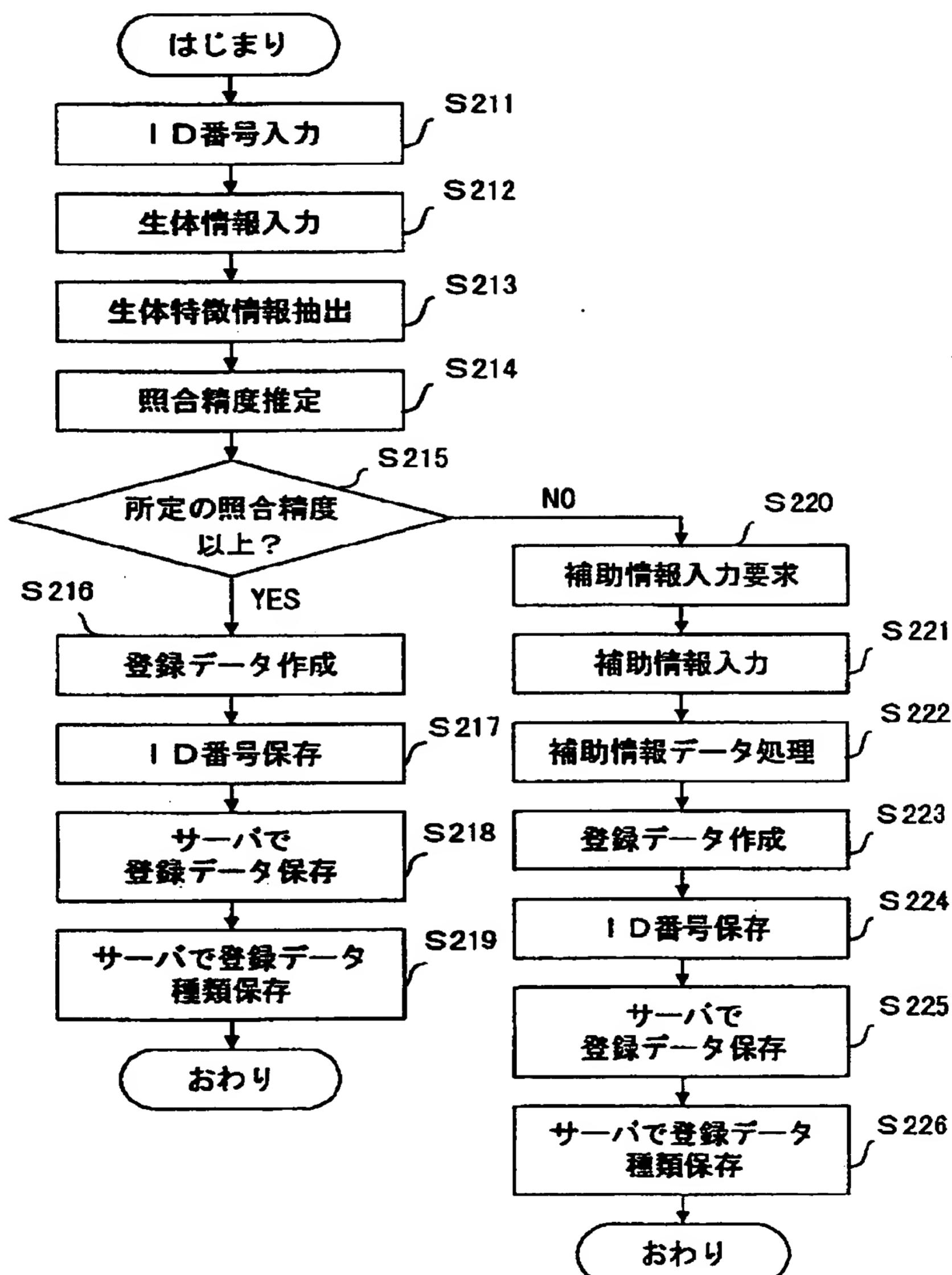
【図25】

第2のクライアントサーバシステムの構成図



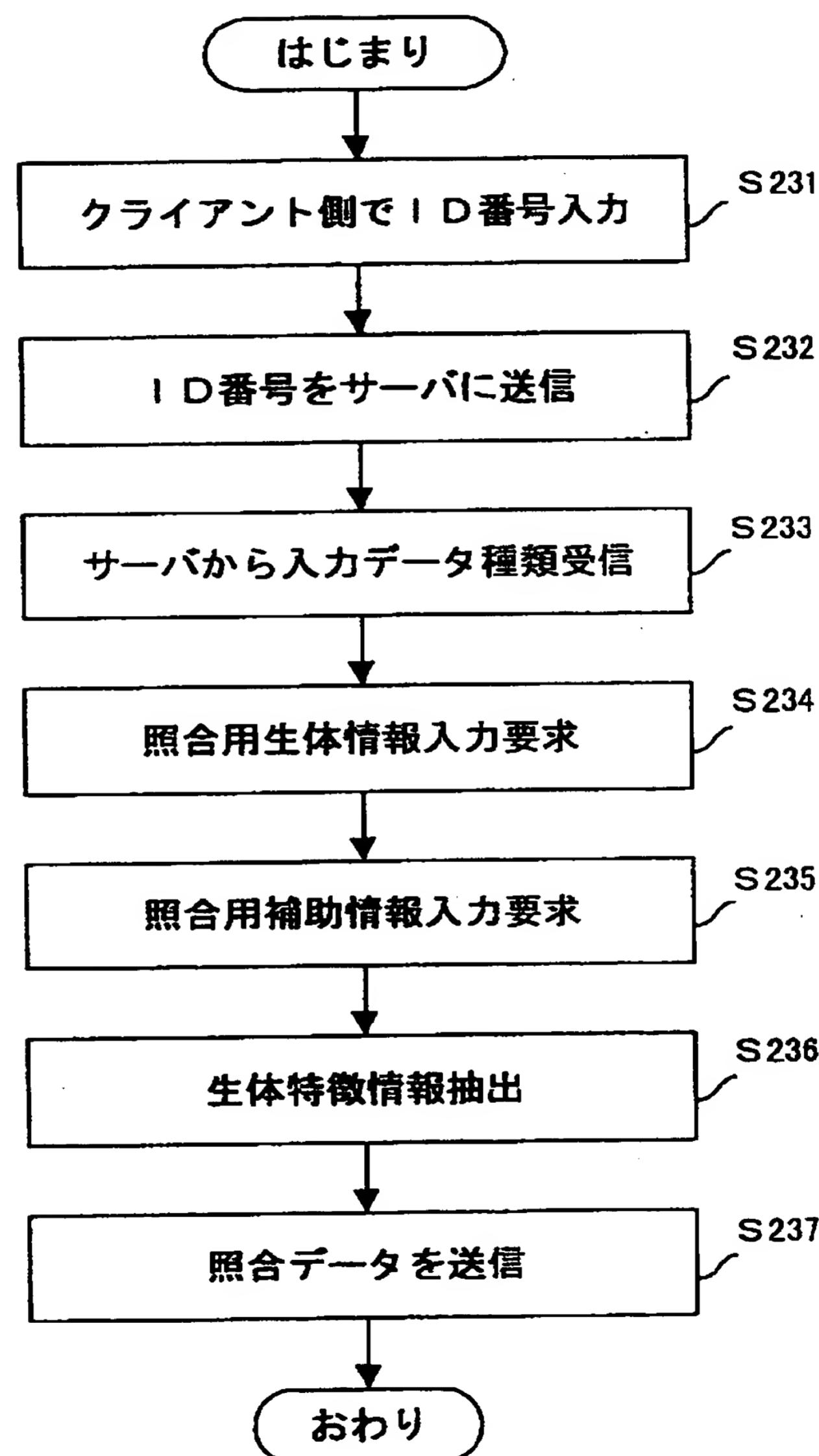
【図26】

第3の登録処理のフローチャート



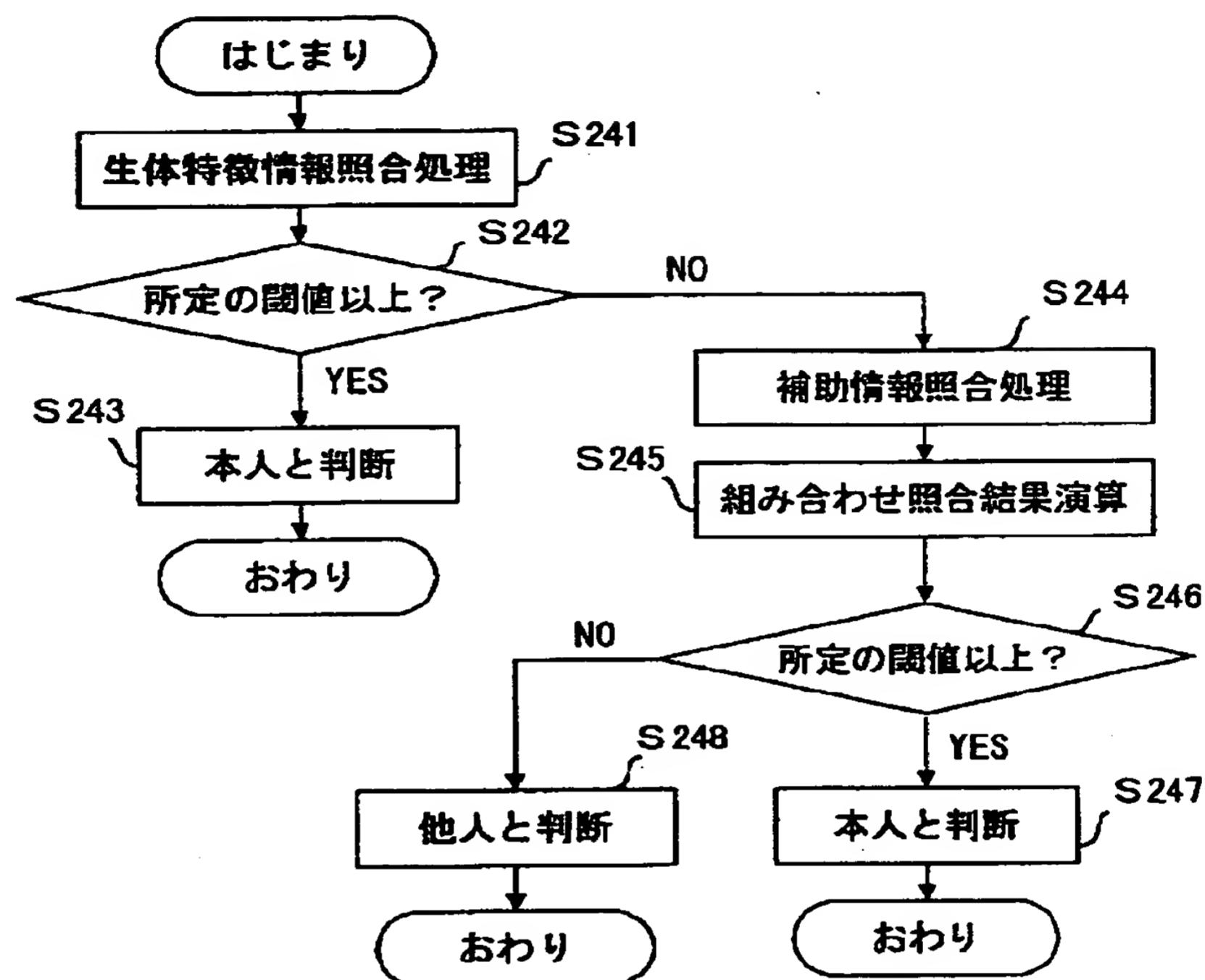
【図27】

第2のクライアントの処理のフローチャート



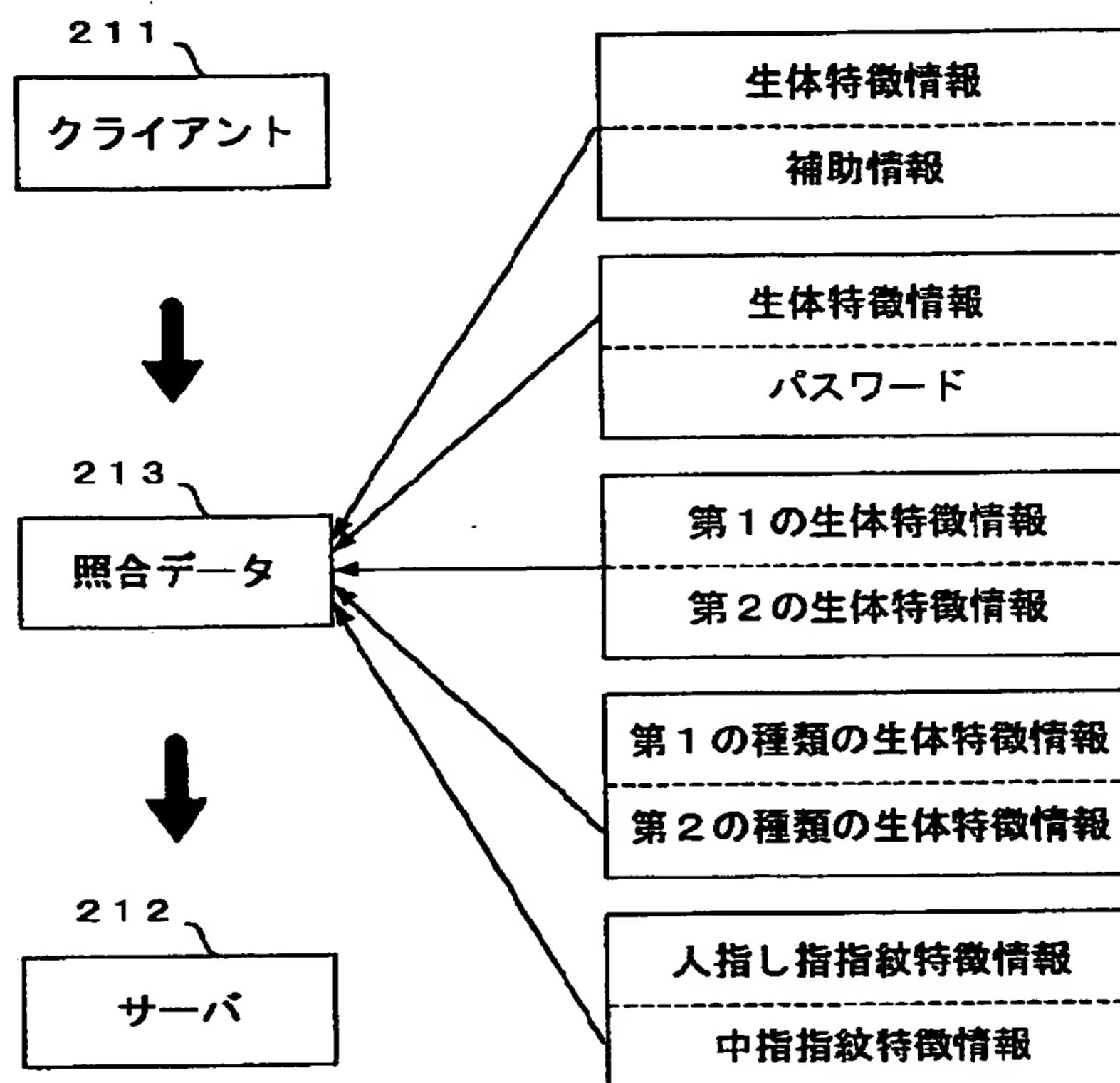
【図28】

第3のサーバの処理のフローチャート



【図29】

照合データの組み合わせを示す図



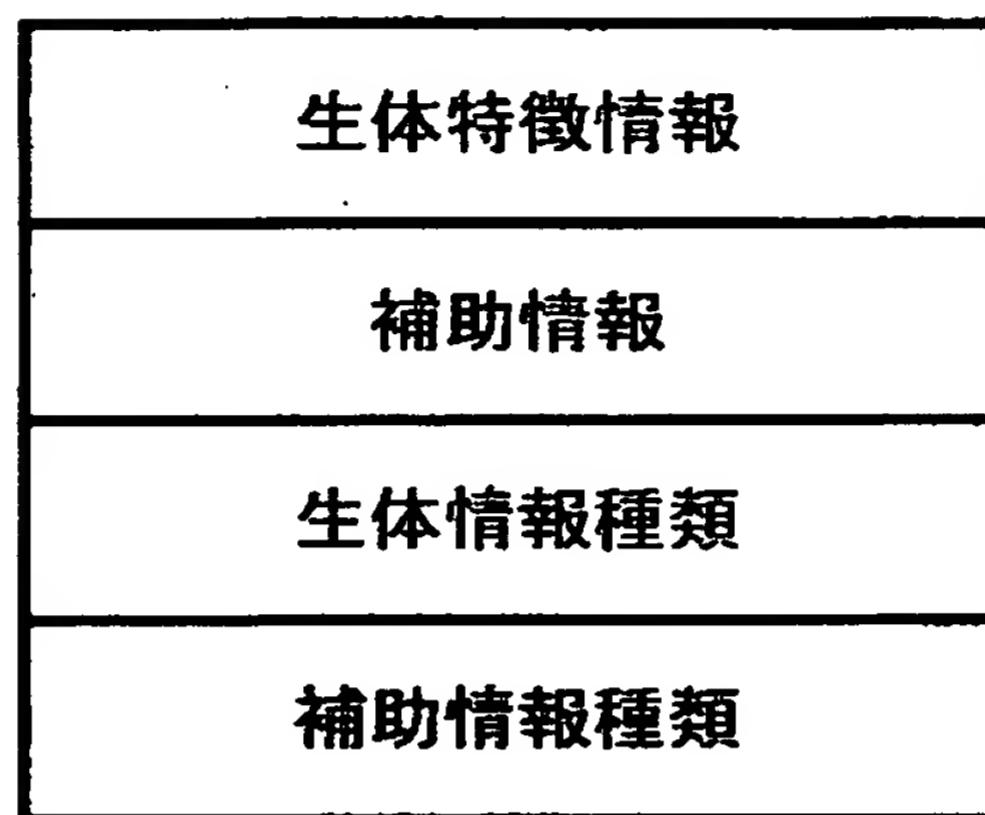
【図30】

I D 番 号 を 示 す 図



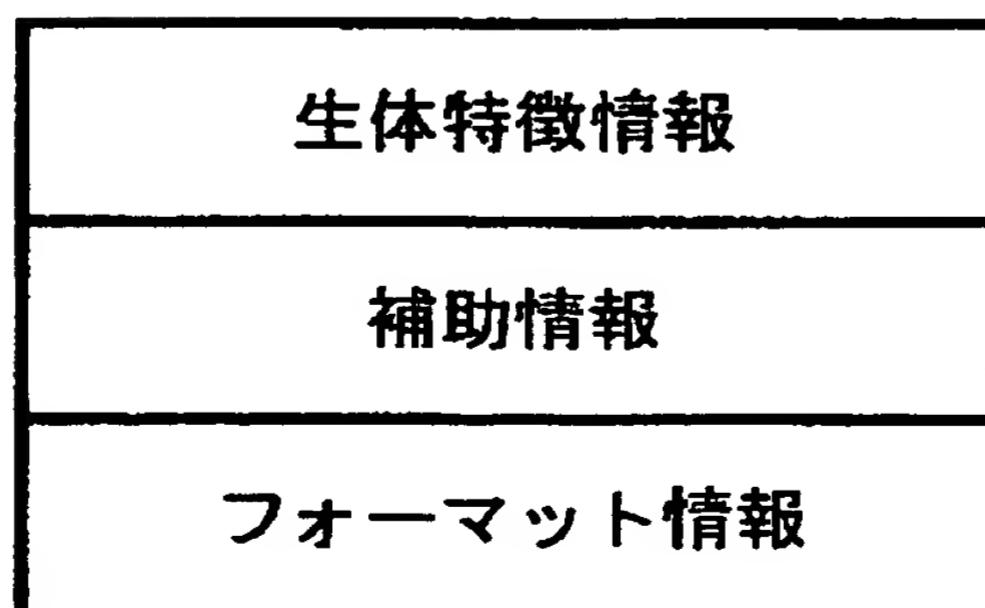
【図31】

第2の
照合データを示す図



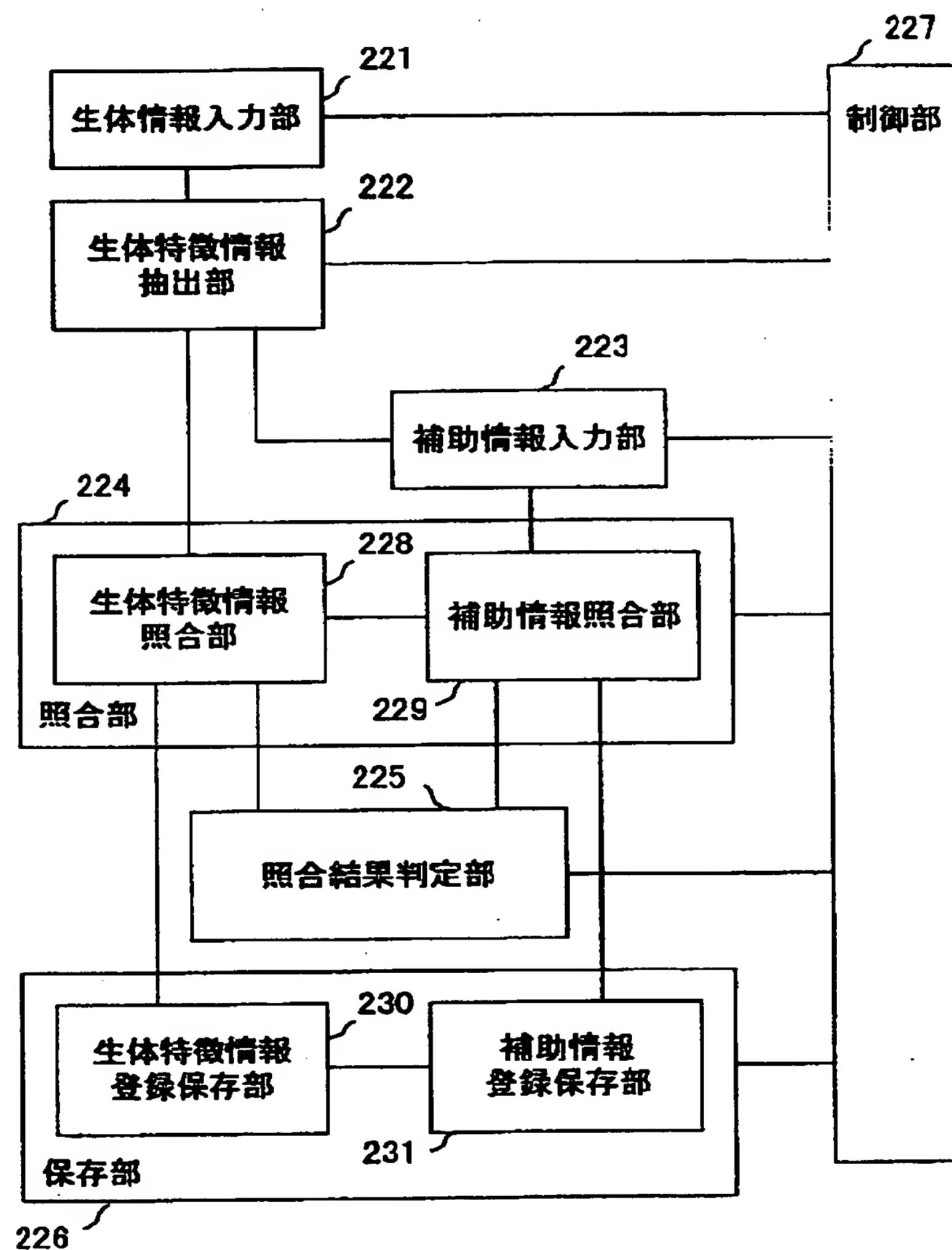
【図32】

第3の
照合データを示す図



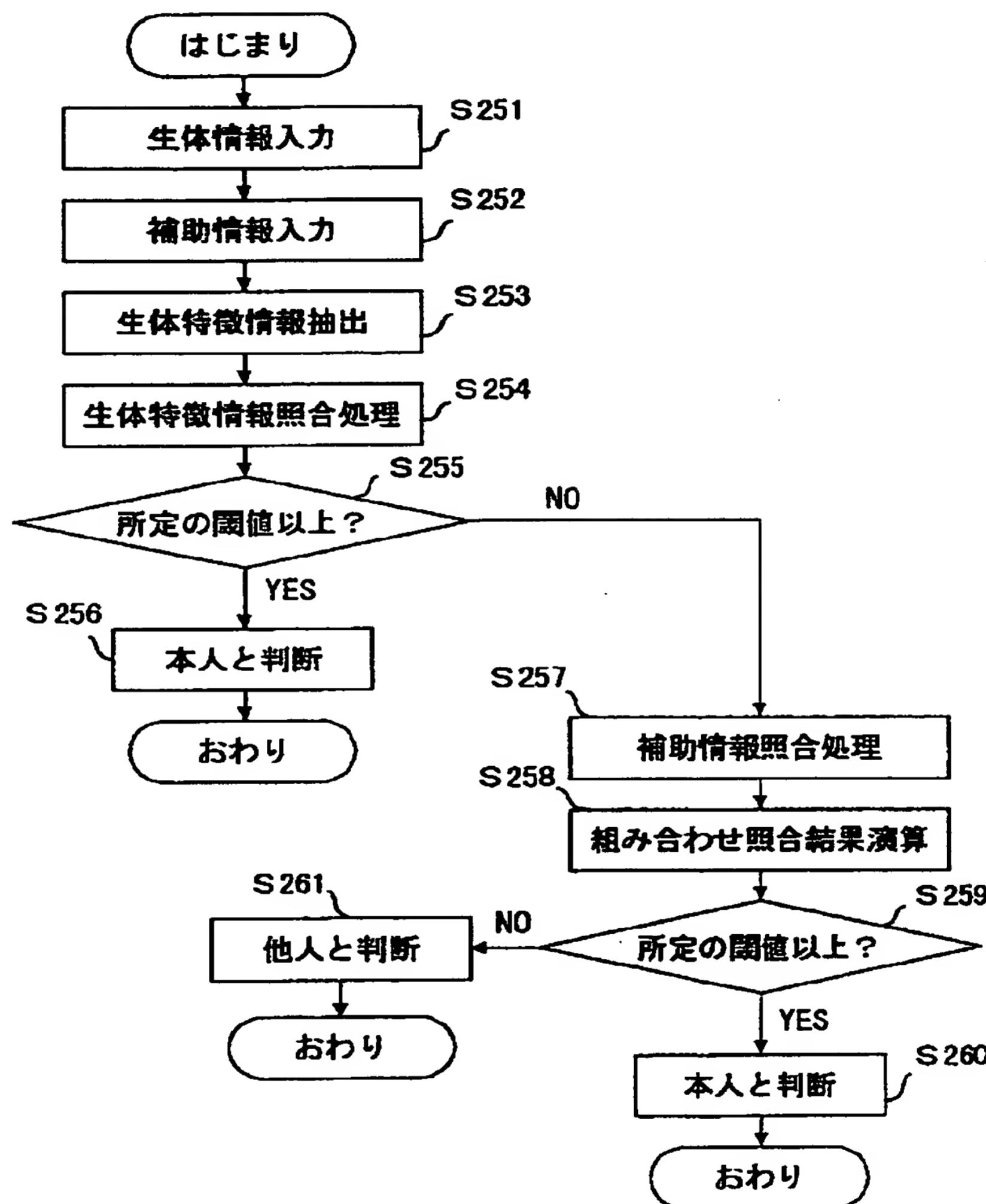
【図33】

第8の認証装置の構成図



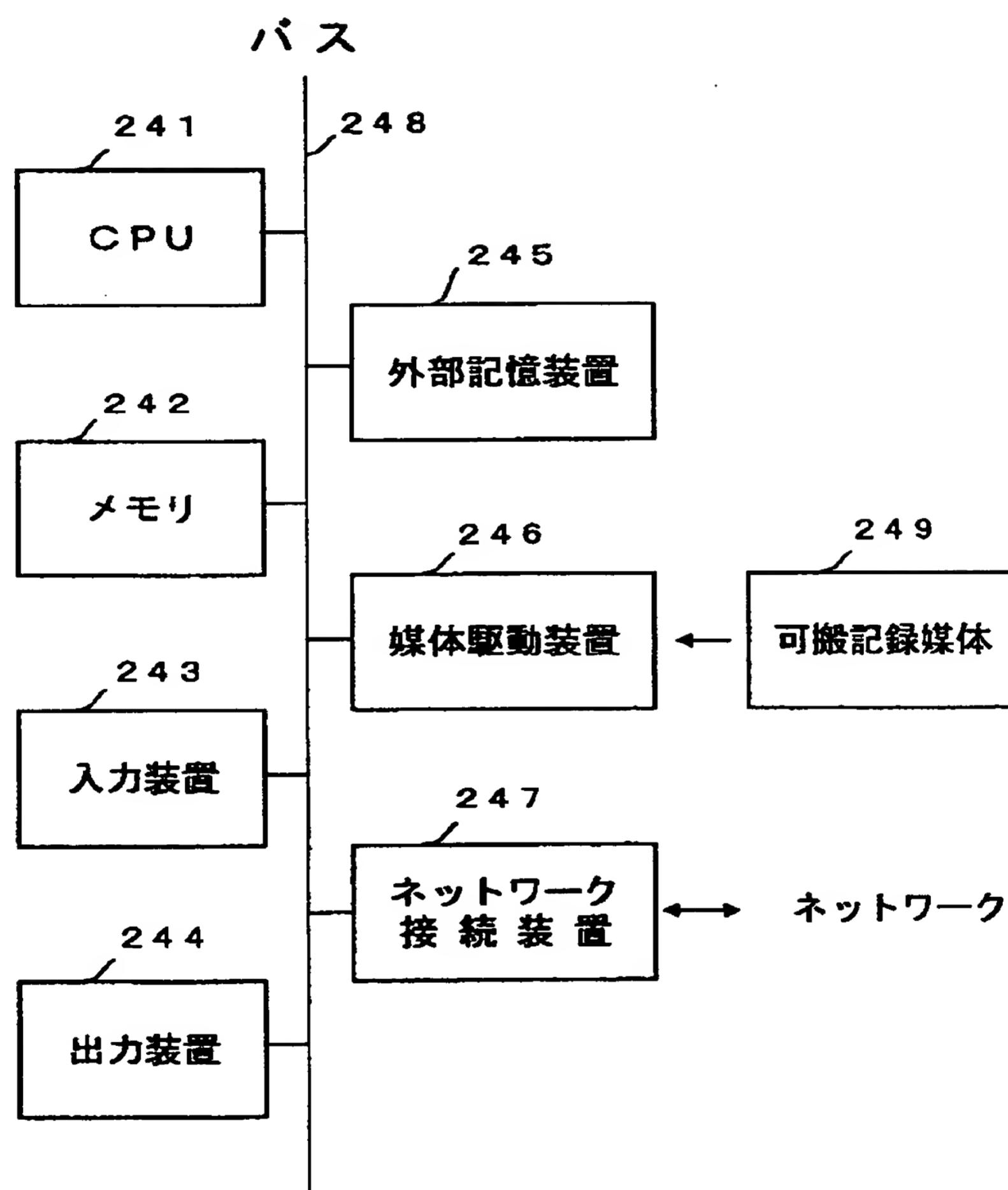
【図34】

第7の認証処理のフローチャート



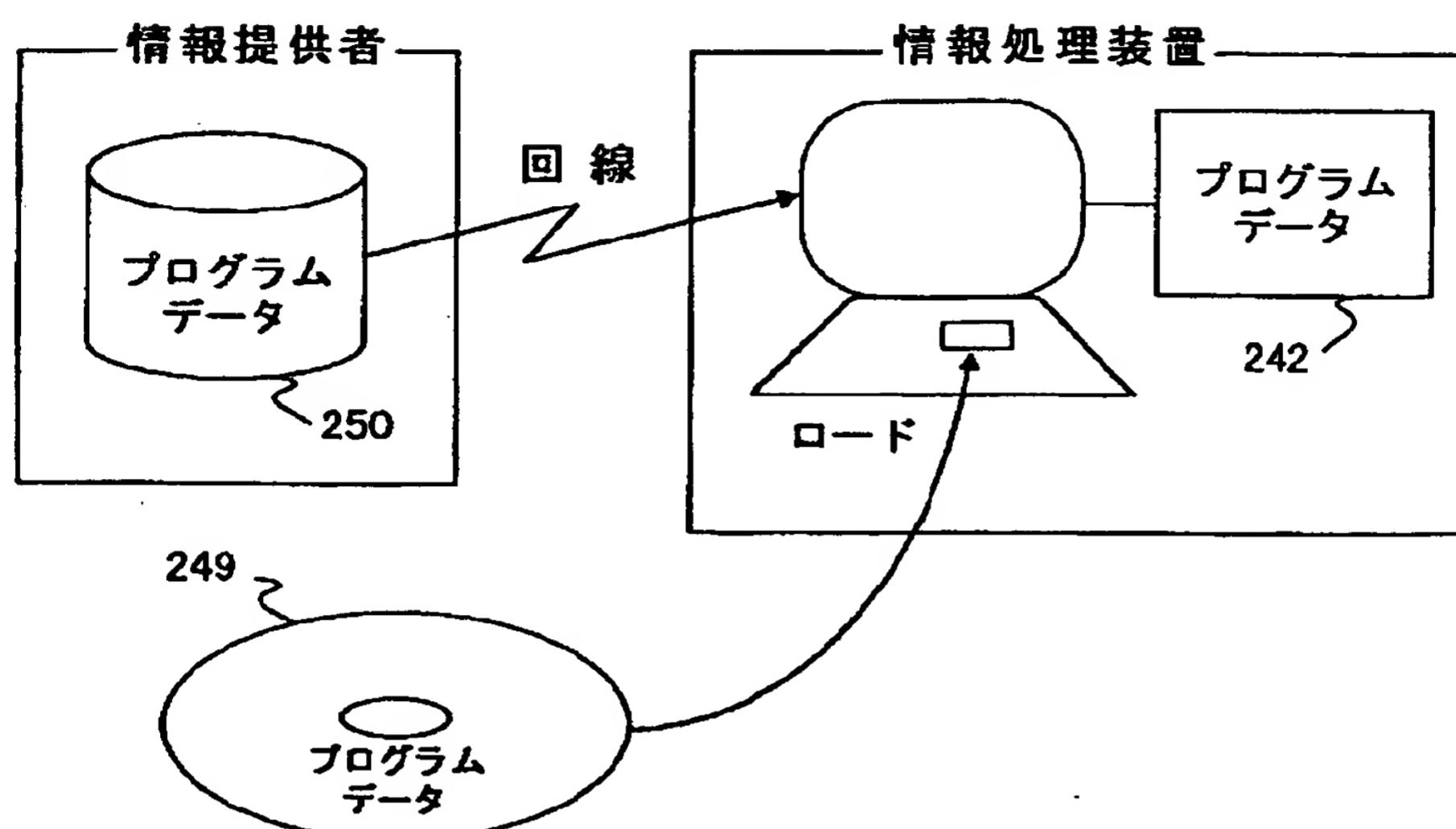
【図35】

情報処理装置の構成図



【図36】

記録媒体を示す図



【書類名】 要約書

【要約】

【課題】 生体情報を用いた個人認証技術において、生体情報の精度が悪い場合でも認証を可能にすることが課題である。

【解決手段】 照合精度推定部13は、生体情報から抽出された生体特徴情報の照合精度を推定し、所定の精度が得られない場合は、補助情報設定部14が補助情報の入力を要求する。照合結果判定部17は、生体特徴情報の照合結果と補助情報の照合結果を組み合わせて照合精度を計算し、計算結果に基づいて認証を行う。また、補助情報の代わりに他の生体情報を入力し、複数の生体特徴情報の照合結果を用いて認証を行うこともできる。

【選択図】 図2

出願人履歴情報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社